Comments to Kelisec's method for generating an encryption/decryption key

Abstract

This report is based on public information on Kelisec's method for generating a one-time, symmetric encryption /decryption key. Beside the communicating nodes, here called Node A and Node B, Kelisec's solution also include a Central Server that holds the information that can be regarded as a seed for the one-time key. The final shape of the one-time key is then decided mutually between Node A and Node B. With Kelisec's method, the Central Server contains no information of the final shape of the one-time key being used when Node A and Node B starts to communicate over the encrypted channel.

1: Background

Kelisec has approached Acreo AB with a patented method for distribution of one time keys for symmetric encryption/decryption. Acreo AB has read the available documentation which consists of a number of patents, see [1]-[4]. This report summarizes Acreo AB's comments to the method.

2: Comments

The basic idea with Kelisec's method is not to send the one-time key as such, just the data needed to generate it. The data is also sent in a way so that only Node A and Node B that has knowledge of the final shape of the one-time key.

The session starts with Node A sending a request to the Central Server to set up an encrypted session with node B. After authority check the Central Server sends a 1st file to Node A containing the "seed" for the one-time key. At the same time the Central Server also prepares a 2nd file, different from the 1st file, that also contains the same "seed" for the one time key. This second file is later sent to Node B. See the representative drawing in chapter 4 for further details.

In Kelisec's solution, Node A and the Central Server possess a "shared secret" which enables Node A to read the "seed" inside the 1st file. The same yields for Node B and the 2nd file. Node A cannot extract the "seed" from the 2nd file and Node B cannot extract the "seed" from the first file. Still it is essential that the communication between the Central Server and the Nodes are executed over secure or encrypted channels to prevent an attacker to log traffic data and run a statistical attack on the "shared secret" or on the "seed". With Kelisec's method, the "seed" and the "shared secret" can be kept unchanged for a number of communication sessions between Node A and Node B.

The final shape of the one-time key is then decided from information Node A and Node B interchange between each other.

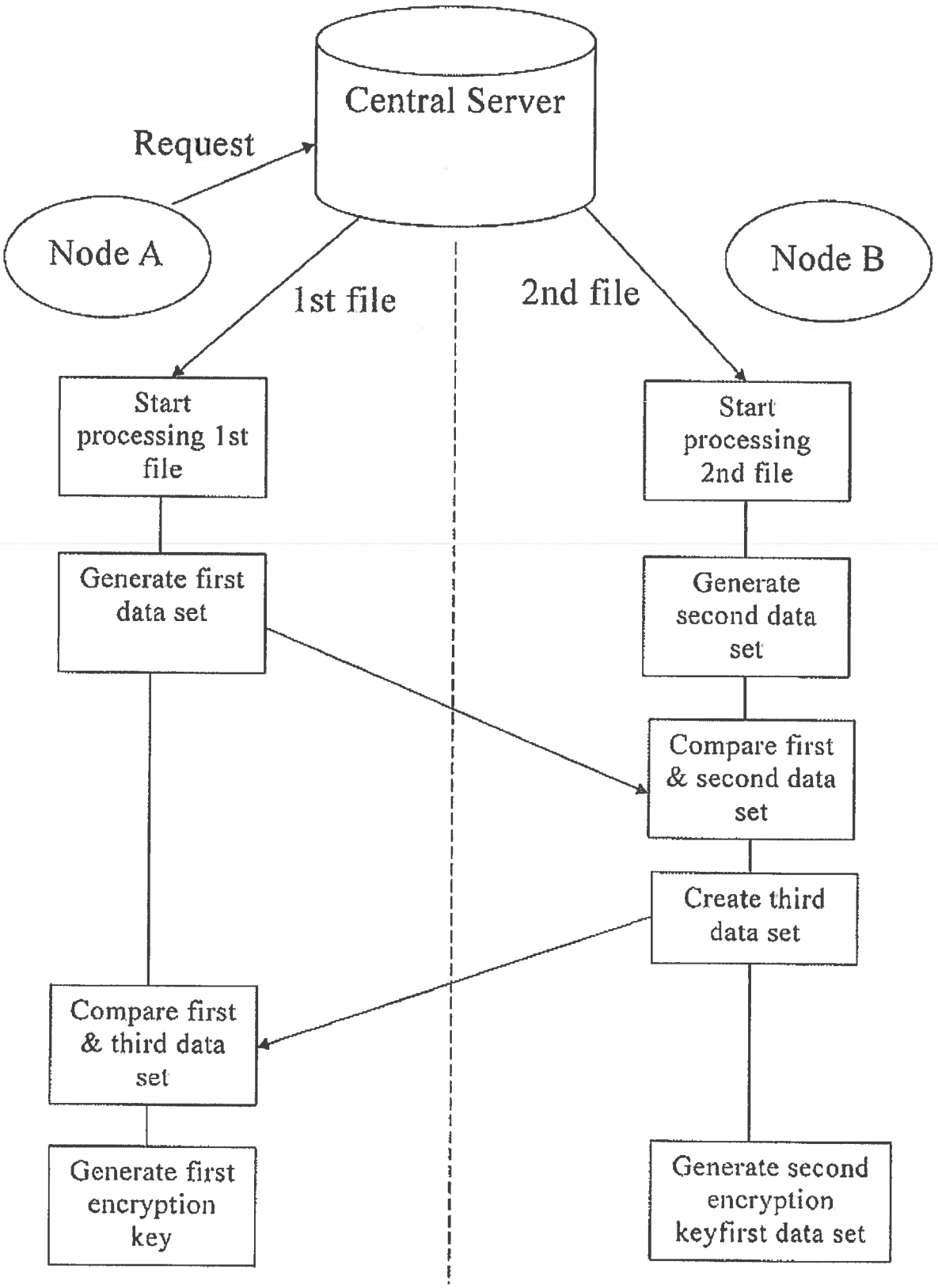
When Node A and Node B has received their files and extracted the "seed", Node A creates a "first data set" and Node B creates a "third data set". Both data sets are transmitted to the opposite Node. Both data sets, i.e. the "first data set" and the "third data set", can be random bit sequences which have nothing to do with the "shared secret" or the "seed". However, it is still desired that these communications also are executed over secure or encrypted channels. See the representative drawing in chapter 4 for further details.

When the data set has been exchanged, Node A and Node B can construct the one-time key with use of the "seed" they had acquired from the Central Server and start to communicate with this one-time key on an arbitrary channel.

3: Conclusions

Kelisec propose a method to distribute and generate a one-time key for symmetric encryption/decryption. The method itself is sound and can be made secure. The level of security for the key distribution obtained with Kelisec's method depends on the integrity of the communication channels between, in the first place, the Nodes and the Central Server and, in the second place, between the Nodes themselves.

4: Representative drawing



5: References

[1] Elise Revell, Kelisec AB,
SE 534 384 C2,
"*Förfarande för att alstra en krytperings-/dekrypteringsnyckel*",
3 July, 2009.

[2] Elise Revell, Uraeus Communications System AB,
WO 2011/002412 A1,
"*Method for generating an encryption/decryption key*",
3 July, 2009.

[3] Elise Revell, Kelisec AB,
CA 2747891 A1,
"*Method for generating an encryption/decryption key*",
3 July, 2009.

[4] Elise Revell, Kelisec AB,
US 2012/0087495,
"*Method for generating an encryption/decryption key*",
3 July, 2009.

(1)-(5)

Implementing the kelisec key "distribution" method.

Mats Poromaa

2012-03-25