h e p i a
Haute école du paysage, d'ingénierie et d'architecture de Genève

INIT
Institut d'ingénierie informatique et des télécommunications
Rue de la Prairie 4
CH-1202 Genève

Tél. +41 (0)22 546 24 00
Fax +41 (0)22 546 24 10

hepia@hesge.ch
www.hesge.ch/hepia

SwissQuantum

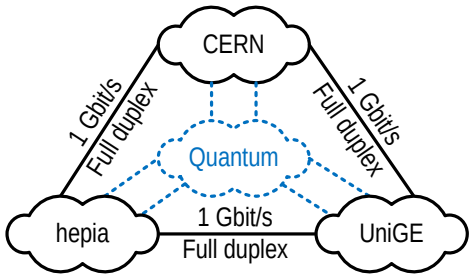
Acronyme: SwissQuantum

Type: HES-SO

Dates approximatives: du 01.07.2008 au 10.10.2009

Coût estimatif total : 276 kCHF

Coût estimatif hepia/INIT : 138 kCHF



Partenaires

- Société Id Quantique (Genève, Suisse)
- HES-SO (**hepia** - leader , EIA-FR, HEIG-VD)
- Université de Genève (Suisse)
- Banque Pictet&Cie (Genève, Suisse)

Résumé

Des établissements (FR-GE-VD) de la HESSO ont collaboré avec la société IdQuantique pour valider dans la durée des échanges chiffrés entre 3 sites (hepia-CERN-UniGE) du canton de Genève. Rappelons que la confidentialité obtenue lors d'un payement sécurisé est basé sur le chiffrement des données à partir d'un secret partagé par les 2 extrémités que nous appellerons Alice et Bob. Il existe diverses méthodes plus ou moins sûres pour permettre à Alice de transmettre ce secret à Bob. La technologie développée par l'équipe du professeur Nicolas Gisin (UniGE) et commercialisée par IdQuantique utilise les lois de la physique quantique pour générer aux deux extrémités ce secret sans qu'il ne soit transmis sur la fibre optique reliant Alice et Bob.

Le travail de l'éventuel espion appelé Charly, consistant à écouter le flux de données chiffrés pour le décrypter, est rendu encore plus difficile si ce secret change fréquemment (chaque minute).

HESSO a d'abord défini un contexte applicatif qui simule les besoins d'un client potentiel tel qu'une banque répartie sur 3 sites pour proposer une architecture redondante capable de faire face à la panne d'un lien intersites tout en garantissant certaines classes de trafic. Cette validation avait aussi comme objectifs de montrer que les opérations de chiffrement (Alice) et de déchiffrement (Bob) ne pénalisaient pas des paramètres tels que temps de latence ou débit utile. Le côté innovant de ce projet a été apporté par l'adaptation du système Linux (IPSec) à être compatible avec les clés (secrets) générés périodiquement.

Contact hepia

Gérald Litzistorf (gerald.litzistorf@hesge.ch)