

## NSA and GCHQ Reportedly Stole SIM Card Encryption Keys

February 20, 2015

By: Denise Sullivan Cloudwards

<http://www.cloudwards.net/news/nsa-and-gchq-reportedly-stole-sim-card-encryption-keys-6481/>

A recent report [shows](#) that the National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) are responsible for stealing SIM card encryption keys in 2010. The latest report draws from information leaked by Edward Snowden, former NSA contractor.

## Gemalto Not Involved in SIM Card Encryption Heist

According to the [report](#), both agencies obtained encryption keys from the Dutch security firm, Gemalto. Since the revelation, the firm has denied knowing about any hack to obtain the information. The group has issued a statement saying it has been unable to corroborate the information contained in the announcement, but it is taking the matter seriously. Paul Beverly, Gemalto Executive Vice President said,

“I’m disturbed, quite concerned that this has happened. The most important thing for me is to understand exactly how it was done so we can take every measure to ensure that it doesn’t happen again, and also to make sure that there’s no impact on the telecom operators that we have served in a very trusted manner for many years.”

Apparently the theft of SIM card encryption keys was in order to allow both agencies access to private mobile phones as part of their surveillance. The report indicated that the hack gave both governments access to a large portion of global cellular communication.

## NSA and GCHQ Cyberstalked Employees

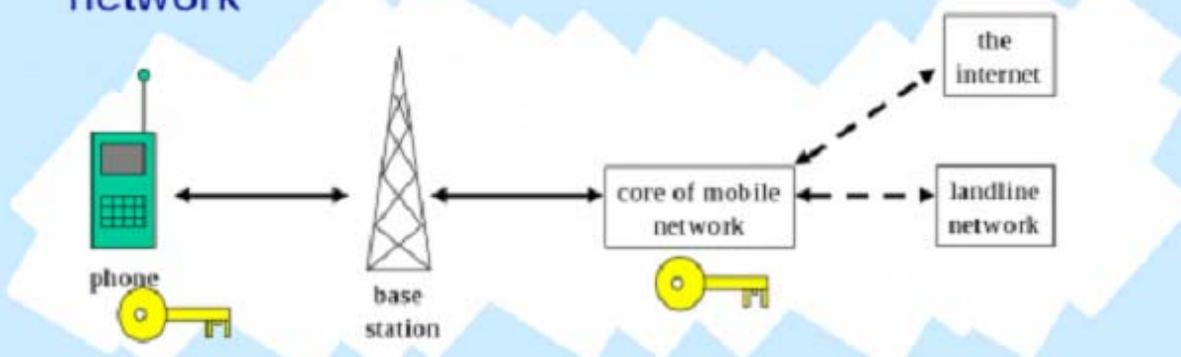
When a SIM card is encoded it contains an encryption key that must be passed to the mobile company in order for it to work properly. This information is sometimes transferred via traditional mail routes such as FedEx or DHL. More often, however, it is transmitted electronically through email or File [Transfer](#) Protocol (FTP).

The SIM card encryption keys were reportedly taken after the agencies monitored Gemalto employees private communications. By hacking email and Facebook accounts they were able to cyber stalk workers to discover who had access to the information and where to get it.

## TOP SECRET STRAP 1

### Where are these keys?

- Keys live on the SIM card in the phone
- They also need to be present on the mobile network; are kept carefully protected in the core network



CCNE "We penetrate targets' defences."

Slide Explaining How SIM Cards Work image credit: [Intercept](#)

For now, neither the [NSA](#) nor the GCHQ are commenting on the latest report. However, some members of Dutch Parliament are calling for a response to the allegations. Should they turn out to be true, both agencies have violated Dutch privacy laws and could be held accountable.

This is just the latest in a long series of revelations from Snowden's accounts. Tell us what you think about the reported hacking of SIM cards.