Comment regarding ”Paper III: Lessons from the Norwegian ATM system” and ”Main Thesis, chapter 4.3”

Written by: Geir Bonde, Bankenes Standardiseringskontor, BSK
Date: 2007-08-06

The disputed incident took place in Spain. The Norwegian ATM system, technically an integrated part of the Norwegian system for handling card transactions - BankAxept, is a national system and will only function with a Norwegian bank as the retailer’s bank. No such ATM existed in Spain on the time of the incident.

The misused card was cobranded; BankAxept together with an international brand. It was the security level on the international part of the card that was disputed in the court. The discussion of the security level of the Norwegian ATM system is therefore misplaced, since the BankAxept part of the card was never violated.

The disputed incident took place in 2001. The Norwegian ATM system, BankAxept, has from June 1999 been equipped with TDES (3-DES, Trippel DES) security. The cards where updated in the ATMs from January to June 1999. After June 1999 no card with only Single DES security would function in BankAxept. The banks security experts were aware of the TDES security in the Norwegian ATM system.

The judge was in doubt, but based his decision on an assumption of DES as the security level in the violated system (”… under noen tvil å måtte legge til grunn at …”). Considering this doubt, the judge would probably have spent more time clarifying this issue if he thought it important for his verdict.

“Paper III: Lessons from the Norwegian ATM system” and ”Main Thesis, chapter 4.3” should be read with this in mind.

Reply from the authors of "Paper III: Lessons from the Norwegian ATM system"

Date: 08-20-2007

The authors wrote the paper because they wanted to analyze the described court case. We were particularly interested in determining how the Norwegian banking community's security-by-secrecy policy influenced the trial, and to further establish whether or not a security-by-secrecy policy leads to worse security over time.

We wholeheartedly agree that the ATM system in Spain should have been investigated during the trial. However, the judge decided to concentrate on the Norwegian ATM system. Based on information provided by one of the bank's expert witnesses, he came to the conclusion that this system utilized DES. Since the authors were interested in evaluating the court case, and not the ATM system per se, we naturally decided to analyze the DES-based system assumed by the judge during the trial.

According to the judge's written verdict, the bank's security experts refuted the feasibility of a trivial cryptographic attack on the DES-based ATM system—despite the fact that this attack has been well-known in the international research community for many years. As a result, the experts provided the judge with wrong information. BSK has not disputed this observation in their written comment or during a meeting with two of the authors. We believe the experts' misinformation is a direct result of the Norwegian banking community's security-by-secrecy policy, which prevents experts from discussing the cryptographic properties of the ATM system with the international research community.

During our research, we chose to follow well-established judicial methodology mandating that an evaluation of a court case should be based on well-documented sources, and not undocumented claims. After the trial, BSK has claimed that the ATM system utilized triple-DES, and not DES. Independent of this undocumented claim, the experts still provided the judge with wrong information about the DES attack. Thus, we see no reason to change the conclusions in our paper.