SCL The IT Law Community
SCL Forum: Internet
www.scl.org

# The DigiNotar Case: Internet Security is No Abstract Matter

**Nico van Eijk** relates a story that illustrates the dangers associated with digital certificates and suggests improvements to the relevant regime

On 2 September 2011, towards midnight, a bar appeared at the top of television screens in the Netherlands with the announcement of an extra news broadcast at 1 am. Had disaster struck the world? Had the government fallen? Viewers were in for a somewhat surreal scene. Piet Hein Donner, the Minister of the Interior, sitting all by himself at an ordinary little table, read out a statement to the effect that the Internet was no longer safe. But we could rest assured and go quietly back to sleep; adequate measures had been taken. The country was saved!

## DigiNotar

The statement marked the beginning of the DigiNotar affair. (For a more detailed account of the DigiNotar-case and the underlying policy/legal issues, see: A.M. Arnbak & N.A.N.M. van Eijk, Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain, paper presented at the TPRC-conference 2012, http://ssrn.com/abstract=2031409.) It had been rumoured that something was wrong with the 'certificates' used for the authentication of transactions and web sites. This technically complex issue boils to down this: for each web site a certificate is required that proves the identity of the web site operator. These so-called SSL certificates are tested via the browser (the little padlock that is either open or locked). In addition to this type of certificate, there are other types, such as Public Key Infrastructure (PKI) certificates. These PKI-certificates are used in the communication with citizens (tax assessment, implementation of employee insurance schemes and DigiD, the national identification system for transactions between citizens and (local) government), but also by civil-law notaries and bailiffs (eg for entries in the land register). When the certificates get compromised, so called 'man-in-the-middle' attacks (MITM) can take place (see the graphic in the download panel opposite). As early as July, DigiNotar knew that the system had been hacked, but it was not before late August that Govcert.nl, which includes combating cybercrime among its activities, received a report from a German sister organization that something was probably wrong: an Iranian Internet user wanted to surf to Google.com and received a message about a possibly fraudulent certificate.

This got things moving. An independent report confirmed the break-in and soon it became clear that not only the Internet certificates but also the government certificates were at issue. Is it true that we could go quietly back to sleep after Donner's nocturnal statement? The operational management of DigiNotar was transferred, in other words: the government was going to take charge. Secondly, a process was started for a transition to other PKI certificate suppliers in the shortest term possible. The process opted for was one of gradual transition so as to safeguard continuity. Thus, it was arranged with Microsoft that the browser would not yet be updated to refuse DigiNotar certificates (meaning that possibly compromised transactions between government and citizens were allowed to continue).

The telco-regulator OPTA swung into action too. By virtue of the Dutch Telecommunications Act (Telecommunicatiewet) OPTA is charged with supervising 'qualified certificates' (also called 'digital signatures'). The PKI certificates at issue belong to these regulated certificates. Providers are to register with OPTA and have a legal obligation to comply with all kinds of regulations. OPTA may decide to withdraw the registration. This happened in the DigiNotar case. Its registration was terminated with effect on 14 September, and DigiNotar was held to withdraw the qualified certificates that had been issued within 14 days. Both DigiNotar and the civil-law notaries and bailiffs

contested the OPTA decision before the judge in interim injunction proceedings, but to no avail. Meanwhile, DigiNotar had already been declared bankrupt. Even today, some DigiNotar certificates are still in use.

## What do we learn from the DigiNotar affair?

The affair was triggered by corrupt SSL certificates, the type most frequently occurring in everyday Internet use. Yet, these are the very certificates that are hardly restricted by a legal framework. They are not among the qualified certificates that are subject to electronic signature regulations. It remains doubtful if there was (or could have been) sufficient awareness of this fact when the European Directive on electronic signatures was finalised in 1999 (Directive 99/93/EC, OJ L 13/12 of 19 January 2000). That Directive is the basis for the provisions of the Telecommunications Act.

The measures actually taken, such as the operational take-over of DigiNotar and the migration to secure certificates, raise a number of questions. Did the government act in a public-law or a private-law capacity when DigiNotar was taken over? The former seems to be the most obvious option, which makes the lack of a legal basis all the more interesting. Secondly, there have been some legally interesting complications with respect to the migration. How were the interests between guaranteeing continuity on the one hand and the risks associated with possibly compromised certificates on the other hand assessed (a question that could also be asked with respect to the postponement granted by OPTA)? And what is the significance of the discussions between Donner and Microsoft on delaying the processing of the compromised certificates?

## What action should be taken?

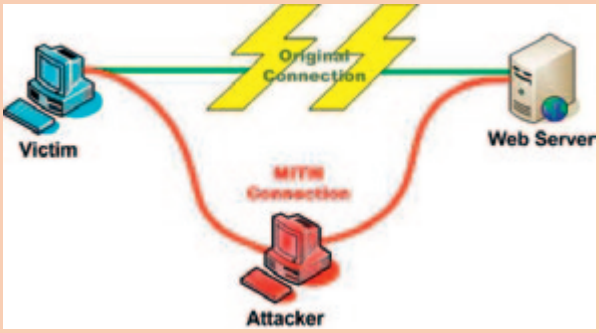
The DigiNotar affair has brought home the fact that Internet security is no abstract matter and that violations may have dire consequences. It is a lesson that is not confined to the Netherlands. Certificates should offer certainty as to web site access and executing transactions. The situation becomes even more critical due to increasing dependence on the Internet and the lack of any alternatives.

A sound analysis and further studies are absolutely necessary; getting back to the old order is no longer an option. Is the system of digital signatures, which was brought about at a time when the Internet was not as ubiquitous, sufficient? Is poor compliance the actual problem and, if so, can tighter supervision provide a solution, or should the whole system go by the board and be replaced by (say) licensing? The proposed Regulation on 'electronic identification and trust service for electronic transactions in the internal market' (European Commission, COM(2012) 238/2), which is supposed to replace the directive on electronic signatures, will not solve the systemic failures of the DigiNotar-case. It mainly brings SLL-certificates under the same framework as the already regulated qualified certificates, but does not deal with most of the known vulnerabilities as such.

I believe we should address the issue rather from the perspective of risks and look at 'critical' certificates that should be subject to specific conditions. Such conditions would apply to the issuing parties (introducing more specific quality of service-criteria), possibly in combination with an obligation for market parties – such as web sites and services using SSL – to use secure certificates from qualified suppliers. In short, the legal framework that is still focused on some classic parties in the value chain between information providers and customers should reflect this value chain in its entirety better – with due observance of such activities as issuing certificates and the role of browsers.

Authorisations and enforcement measures also call for critical analysis. The DigiNotar affair lacked a legal foundation with regard to essential steps. The take-over of operational processes and negotiating with market parties with respect to public-law interests – as took place between the Dutch government and Microsoft – should be embedded in legal context, not least to enable adequate action and prevent abuse. In the DigiNotar-case it became clear that even the safeguards based on regulated certificates did not work: alternatives might be necessary. Finally, with respect to the measures taken, the interests should be assessed more transparently, and it should be clear how transitional measures relate to the risks (and possible liabilities). ●

The unauthorised issuing of SSL-certificates creates the possibility of 'man-in-the-middle' attacks (MITM). The Open Web Application Security Project (OWASP)-web site (https://www.owasp.org/index.php/Man-in-the-middle_attack) describes and illustrates these attacks as follows: *The man-in-the middle attack intercepts a communication between two systems. For example, in an http transaction the target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the client and the attacker and the other between the attacker and the server, as shown in the figure. Once the TCP connection is intercepted, the attacker acts as a proxy, being able to read, insert and modify the data in the intercepted communication.*




**Nico van Eijk is Professor of Information Law, in particular of media and telecommunications law, at the Dutch Institute for Information Law (Instituut voor Informatierecht, IViR, of the University of Amsterdam: www.ivir.nl/staff/vaneijk.html).**