6

The Role of Government in creating the IT security infrastructure

Builder or bystander?

by Mads Bryde Andersen
Professor of Law, dr.jur.
University of Copenhagen
Denmark

Abstract

The author of this paper has been the chairman of the Danish IT Security Council since it was established in 1995. He has also worked closely with the Ministry of Research and Information Technology on a Danish draft act on Digital Signatures. The paper reports of some *political* experiences in creating an IT security infrastruture; experiences which might very well also be envisaged by other countries. It does not necessarily reflect the views of the IT Security Council or the Danish Government.

The need for an information infrastructure

To implement certain information security solutions you need an information security infrastructure. In an open environment, encryption and digital signatures can only be applied on the basis of a trusted third party infrastructure consisting of certification authorities, key centres etc. Furthermore, certain security measures will only be trusted, if users have confidence that they are using systems which have been okayed by public entitites.

This opens the question of what roles Governments shall have. Broadly speaking, Governments can either play an active role in *building* up such an infrastructure, or they can sit passively as *bystanders*.

First and foremost, Governments can play actively as *law-makers*, setting up the substantial and procedural rules for communicating parties and for the private entities who want to undertake the jobs as certification authorities. As a part of such schemes,

Governments could also be *controlling entities* that authorize private entities to undertake certification authority functions. Government entities could even undertake the role as *trusted third party*. By doing so, Governments play the job of a *builder* of the information infrastructure.

But Governments could also chose a more passive role as a *bystander*, waiting to see what solutions are brought forward by industry, and only interfering if substantial risks are at stake. Indeed, this role appears to be the easiest one, at least in the short run. Due to its immaterial nature and to the complexity of information technology, information is one of the most complicated issues to regulate by law. Politicians are often confused when it comes to questions of "information legislation" (be it data protection laws, "decency" legislation or encryption policy), and information policy processes are therefore difficult to manage and predict. When it comes to personal information - which most information is - the questions also touch upon fears of the unknown. This is mainly due to the unpredictable ways by which information can be used against individuals. Therefore, it is easy to understand why some politicians prefer the role of a bystander; a role which may even be justified by the modern trend of market control and competition in the information industry.

The Danish experience - an example

Denmark presents an example that other countries might be able to learn from when it comes to discussions on the Government's role in building an IT information infrastructure. Denmark is a rather small country with approximately 5 million citizens, but Denmark has a relatively large public sector which has made extensive use of computer technology for decades. Denmark also has a financial sector with a strong tradition for co-operation on IT issues. Within this sector, it is the general attitude not to compete on IT security matters. All Danish citizens have a unique personal identification number (the CPR-number, Central Personal Register) which is used to identify individuals both for governmental purposes (taxation, social security etc.) and for private purposes.

To add to this, Denmark has substantial expertise in the field of the technological applications and the legal implications of cryptology. The Danish company Cryptomathic A/S, founded by Professor Peter Landrock, has provided cryptographic solutions both to public entities and private enterprises for a number of years. In law schools at the universities of Aarhus and Copenhagen, legal scholars are working with contractual and other issues regarding the use of digital technology.

This explains, at least partly, why Denmark also has an early history of considering public key infrastructure issues. As early as 1989, a Danish Teletrust group was created on a private basis by the Danish Data Association to discuss how a Danish "Teletrust" scheme could be established. The group presented its findings in 1991: A government-based control key centre authority, referred to as a CCA - Centre Certifying Authority, should be formed for key centres. The CCA should certify and control key centres and thereby provide a more solid legal basis (e.g. in relation to liability issues) for that new and hitherto unknown kind of business.

Based on the Teletrust proposals, The Danish Telecommunications Agency appointed a working group in the beginning of 1992 to consider how to implement the Teletrust proposal into real life, cf. my article in The EDI Law Review, vol. 1, no. 1, 1993, pp. 43-53. However, the subsequent development proved to be less visionary and certainly more reluctant. It became difficult to gain the Government's support for the proposal: Why should the Government be engaged in the creating of new regulatory infrastructure when the involved industries had not taken any initiatives. Could the intended results not be reached by other means?

As indicated in my above article, it is easy to see the arguments against setting up such a framework. One argument put forward was that the time has not come yet for a small country like Denmark to enter that path. Another, that there were already legislation in force that would make certification of privately held key centres possible, namely the rules providing for a general certification and accreditation scheme dealing with the accreditation and certification as part of a quality assurance concept (however, without specifying the basis for such accreditation and certification).

The political winds around this issue changed dramatically in 1994. Since then, the Danish Government has put information policy and IT security on the top of the political agenda. The idea of creating infrastructures for public key-based communications was invoked in 1994 when a report by the Danish Government was published, "Info-Society 2000". In this visionary report, a long list of proposals for bringing Denmark into the Information Society was made. Subsequently, the Danish Ministry of Research and Information Technology has worked intensively to implement the suggestions from the Info-Society report, and other suggestions have been made and implementing, among them the setting up of a Danish IT Security Council and the proposals for Danish digital signature legislation.

The various roles of Government

As this short presentation indicates, Governments *can* take various different attitudes towards building the IT security infrastructure. Governments do not necessarily have to act as builders. They may very well chose the role of the bystander, while at the same time supporting the very notion of having such an infrastructure. Before we go deeper into the topic of what particular role, Governments *should* play, it may be useful to take a quick glance backwards in history.

Although the role of Governments has changed dramatically over the last centuries, some functions have remained the same. One of them is the task of providing security for citizens against various *threats*. Most activities Governments engage in concern the safety and well-being of individuals and enterprises. Health care, environmental protection, traffic regulation, product safety regulations, food and drug administration not to mention criminal investigation and military security are just a few examples of such security functions.

> It is somewhat of a paradox that one of the threats that Government shall protect citizens against, is Government itself! When personal data on citizens are

> processed, a clash of interests occur. The processing itself seems - at least to someone - to turn Government into a "Big Brother". This privacy concern has been the basis for the severe European rules on data protection (cf. European Directive no. 96/46/EC of 24 October 1995). Even though from the outset these rules were aimed at the processing of personal data for purposes of public control, taxation or the like, they also apply in regard to IT solutions provided for computer security infrastructures. A clash between various data protection policies also occurs in the encryption debate. On one side, encryption is one of the most powerful tools to obtain confidentiality of data (and thereby privacy of personal data). Nonetheless, the privacy issue is also raised *against* encryption technologies, because the use of computers to implement encryption solutions implies registration of personal data.

Another important task for Governments concerns the Government as an *organizer*. Governments have a certain obligation to provide for "traffic rules" between individuals and enterprises. Just as important it is to have rules for road traffic, any civilized state must have some basic principles on how citizens shall act towards each other when entering into contracts or other binding relations. Up until now, such rules have mainly been derived from the business practices of a "common law" nature. But presently there is a widespread feeling that in order to foster the use of electronic commerce, specific rules are needed on how to establish legal obligations by means of digital technology.

Last, but not least, in a state with a substantial public sector, there is a demand to provide administrative functions in the most efficient way in order to reduce taxation. Since most public sector activities are financed by taxes, every Government has a natural obligation to apply the most efficient technology in order to reduce costs and enhance services. And obviously, information technology is an important tool to achieve that.

The following three examples will indicate some of the problems faced by the Danish Government in its endeavours to implement new security framework to public administrations and electronic commerce.

The citizen chip card experience

Among the proposals from the Info-Society 2000 report was a proposal already presented by the Ministry of the Interior to create an identification card ("Citizen card") based on public key encryption technology but with other possible features. As the proposal was made, no clear indication was given as to the use of that card, but it was obvious that one of its main features would be to support communication between citizens and Government. The card should provide for digital signature functions and for encryption for confidentiality purposes.

The proposal was met with substantial opposition among people of the kind often referred to as "ordinary citizens" (many of whom saw the proposal as a new way for Government to collect personal data on individuals) and by some politicians (of whom even a significant amount had apparently not understood what the project was about).

The criticism was so substantial that the otherwise technology-favouring Danish Government decided to postpone the final decision on the project.

In September 1995, a new citizen card proposal was introduced. In a new report form the Ministry of the Interior, the chip card should only work as a key combining knowledge on the social security number of the holder and his/her PIN-code. It was strongly stressed that this card would not provide further registration on the card and that no new registers would be made within Government (apart from a log to enable users to *prove* their communication). The main idea was that citizen cards should support communication between individuals and Government, but the card would also be based upon an open architecture allowing for common standards and a coherent infrastructure that might support implementation of digital signatures on a broader scale.

It took only one year before that proposal was also taken back.

In October 1996, the Minister for the Interior decided to postpone the citizen card project. Officially, two reasons were given. One reason was that the operating systems for chip cards of the kind that should be applied in the citizen card were not yet available. It would therefore take considerable time, effort and money to develop the necessary technology for the card. Secondly, it was mentioned that the expected law on digital signatures would have a hampering effect on the citizen chip card project, since the proposal for a digital signature legislation was expected to allow private entities to provide for security solutions for digital signatures. In other words, since the citizen chip card should not be the only technique to provide for this important function, why should the Ministry of the Interior invest such a substantial amount in its implementation?

As it is now, the citizen chip card project is on the "shelf". It is interesting to note, however, that the postponement of this project has effected one of the concerns raised *against* the citizen chip card, namely the concern for the "weak" citizens. In the citizen chip card proposal, citizens would be in a position to obtain a Government sponsored card at a lower cost, if not for free. Now they will face a market of private companies that will offer their services on a profit oriented basis.

The digital signature experience

In the 1996 IT-action plan from the Danish Government, a proposal was included to put forward legislation on digital signatures. Over the summer of 1996, a first outline of a Digital Signature Act was drafted and in the fall of 1996, various hearings were convened to discuss this proposal (and subsequent proposals) with interested parties and industry representatives.

When the question of Government roles is raised, one might ask whether there is a need for such legislation at all. Is it not so, that businesses and individuals who want to communicate by digital means can do so on the basis of contracts?

Under Danish law, the answer to that question is *yes*, if we talk about the relationship between private individuals and if there is no specific obligation to use paper or paper signatures. But when it comes to questions relating to public entities, the power of contracts is limited. If the law requires or assumes that a particular application shall be filed on paper and signed, such a requirement can only be adjusted by way of new legislation. The same problem occurs in areas where regard must be taken to third parties, for example in relation to rules on negotiable instruments.

One of the difficulties in making digital signature legislation is standardization. Digital signatures are made on the basis of digital documents, but digital documents are only used between parties who have already agreed on ways of communication. Without commonly accepted standards for digital communication, it gives no meaning to attach special legal consequences to the digital signatures as such.

This dependency on standards and "codes of conduct" create a circular problem: Without certainty of the legal consequences of digital signatures, it is difficult to implement standards for digital communication on a wide scale. But without such standards, any attempt to draft digital signature legislation runs the risk of vanishing into thin air.

In the first versions of the Danish draft on digital signatures, this "vicious circle" was broken by a proposal that any governmental initiative should be under the obligation to receive digital communication. Such an obligation can only work in relation to public entities. It would not only be politically problematic, but indeed practically difficult to implement. This proposal has not yet been subject to discussions on a broad scale, mainly because its first versions have been restricted. It remains therefore to be seen whether the proposal - that any initiative of the Government should be under the obligation to receive digital communication - will find acceptance.

One might very well assume that this problem has obstructed the digital signature project. Not so. As it appears when this paper is submitted (January 1997), the introduction into Parliament has been delayed by other reasons, namely the problems regarding encryption policy:

The role of investigation authorities

When encryption is used for confidentiality purposes, problems of quite a different nature than those related to communication security arise. Whereas encryption may be used to conceal information, law enforcement and perhaps essential parts of government intelligence activities may be obstructed. Investigating authorities often face difficulties when suspects have locked written communication by encryption, as it is already the common practice among hackers. If encryption is allowed - as it is now in Denmark - criminals and criminal organisations deprive the investigation authorities of one of their most important tools. Therefore, the need for businesses and individuals to secure communication by encryption and the need for Governments to be able to intercept communication have created a confrontation between two valid interests.

The balancing of these fundamental interests has already given rise to political discussions in various international fora as well as to some legislative initiatives. In December 1996, an ad hoc group of experts on cryptographic policy guidelines finalised its work on cryptographic policy guidelines. The December meeting concluded one year of work within that working group, and the proposal will now be brought forward to other fora within the OECD before its final adoption, probably in the middle of 1997.

The Danish IT Security Council has recommended that Denmark should maintain the free use of encryption technology, and that "escrow solutions" should not even be built into those security applications that might be available as a public service (like the former citizen card proposal). Up until now, no formal decision has been taken yet by the Government.

The political marketing issue

Security professionals may find it easy to agree on how to create an IT security infrastructure. But when their conclusions are brought forward in a political process, it often shows that the general public have quite different attitudes. For "ordinary citizens", the very notion that facts are registered within computer systems is subject to much concern. For investigating authorities the need to intercept communication is obviously of high concern.

There is a great risk that the possible roles of Governments in creating an IT security infrastructure is affected by concerns that security people might find less adequate. Therefore, it seems to be an important but somewhat disregarded task for the data security environment to explain things in a direct and clear way to provide for the necessary public support for building an IT infrastructure. This job also includes talking to politicians and Government official to make sure that specific Governmental concern does not lead to unreasonable restrictive policies.