Electronic Administration in Iceland

Páll Hreinsson

1 Introduction

On 7 April , 2003 Act no. 51/2003, amending the Administrative Procedures Act, no. 37/1993 (electronic administration), came into effect in Iceland. The main purpose of the Act was to remove legal obstacles that could prevent administrative cases, in which administrative decisions were to be taken, from being managed entirely *by electronic means*. The Act appended a separate Chapter to the Administrative Procedures Act no. 37/1993, Chapter IX, which describes the necessary minimum requirements to be met with regard to electronic administration.

The following is a brief discussion of the provisions in the new Chapter of the Administrative Procedures Act which addresses the issues of electronic administration. It begins with a short account of the status of electronic government in Iceland and a consideration of the essence of those legal questions that first had to be tackled before establishing a procedure for the electronic handling of administrative cases. This is followed by a discussion on the main principles and assumptions upon which Chapter IX is based. The final section covers the substance of the provisions in Chapter IX on electronic administration with a brief account of their links with other legislation. The provisions contained within Chapter IX of the new Administrative Procedures Act are included in an appendix.

2 Traditional and Electronic Handling of Administrative Cases

As with other Nordic countries, Iceland has embraced information technology on an extensivescale. Computer ownership and Internet usage already rank among with the highest in the world, and the trend is steadily increasing. Thus all external conditions appear to be in place for the systematic employment of IT in the service of the public. Government authorities have set up home pages or websites on the Internet to disseminate all kinds of information to the public. A particular priority has been to communicate practical information on the Internet by granting the public access to databases. For example, the corpus of Icelandic law and the Parliamentary Record have been accessible on the Internet for a considerable time and a centralised Internet database of legal resources was recently opened, where the public can gain access, at one and the same site, to all the laws, regulations and other administrative actions, international treaties, court rulings and final rulings by the authorities that have general application or create a precedent. Various aspects of the internal structure and activities of government authorities have also been addressed. Emphasis, as far as possible, has been on harmonisingsoftware, hardware and procedures within the administration, among other things in order to facilitate electronic communication. To this end, software has been under development for the electronic management of administrative documents, with the aim of equipping the administration, in the course of time, for a phased switchover from a paper-based to an electronic environment, including the submission of electronic documents to the National Archive in electronic format.

From a technical viewpoint, information can be intermediated electronically at any stage in the conduct of a case. An administrative case may begin when a party to it sends notification to the authority through an electronic medium, or the authority can likewise open the matter on its own initiative with an electronic notification to the party concerned. Communications during the actual handling of the case can also be made by means of electronic media. This could include such things as notifications, information and guidance from the authority to a party to the case, and the party's response to the authority. In some instances, the authority might even make an automatic decision using electronic media. The prerequisite for such a procedure for it to be able to serve its purpose, would generally be that the application was submitted to the authority in a specific form and all the conditions for deciding it formalised. The publication of decisions, arguments, and guidelines for appeal could also be done electronically. Finally, all case documents may be stored electronically and transmitted electronically to other parties.

Although computer technology has been successfully used in most areas for facilitating access to information, interactive communications between government authorities and parties to administrative procedures are still largely in their infancy and in general an administrative process cannot yet be completed electronically at the present time. The Icelandic administration has long used paper as the main medium for formal communications, both with citizens and internally. Applications to the administration have thus as a rule been made in writing, and so have decisions made in continuation of them or on the authority's initiative. Nevertheless, most administrative matters over the past decade have in parts been *handled* electronically.

3 Current use of Electronic Communication in Administrative Procedures

While it is rare in Iceland for an administrative case to be managed *entirely* by electronic means , examples have been known. In recent years the customs and excise authorities have taken extensive advantage of electronic media for sending, receiving and processing import documents and facilitating customs clearance. Electronic data interchange (EDI) techniques are used and Act no. 69/1996 made a number of amendments to the Customs and Excise Act, no. 55/1987, in order to strengthen the foundation in law for such administrative procedures. EDI has been applied in two ways: an importer submits a *standardised message* to the customs authorities, and data is sent directly via a closed data network. Regulation no. 858/2000, on EDI Customs Clearance, authorised the transmission of data over the Internet via electronic forms on the Customs and Excise website. Accordingly, importers can now apply for and obtain customs clearance electronically through either a closed or an open network (the Internet), using electronic signatures in the latter instance.

The tax authorities have in recent years enabled electronic submission of VAT reports, tax returns and annual corporate reports via their website, and

reading and processing of tax returns is also largely conducted with electronic media

4 Main Legal Questions in Establishing Electronic Administration

Undoubtedly there are many reasons why IT is only used to a limited extent inhe actual handling of administrative cases. However, its use is probably hindered by various technical obstacles, such as the difficulty of ensuring confirmation of the content, signature and reception of electronic documents compared with written ones. This article will not discuss such technical or organisational problems. It will address only the extent to which there were considered to be legal obstacles to the use of electronic media in handling of administrative cases and the manner in which the provisions of Chapter IX of the Administrative Procedures Act have overcome them..

Legal rules on government administration, both in force and established by tradition, inevitably take customary administrative procedures into account. For this reason it was considered necessary to make a separate study of whether, and to what extent, the distinctive features of IT called for specific rules to be laid down in order to take full advantage of its benefits in administrative procedures. To this end, on November 7, 2000, the Prime Minister appointed a committee to examine these issues. It submitted its report to him on October 10, 2002, with proposals for solutions to the legal problems that it discussed.

The report emphasised that it could not be taken for granted that new technology and new modes of communication, such as the electronic dissemination of information, called for new rules. Rules were inherently abstract and thus not confined *a priori* to real incidents or circumstances. Rules could therefore remain fully valid even if circumstances changed and new technology evolved. Accordingly, the bulk of the administration's procedural and material rules were technically impartial and applied irrespective of whether communications had taken place electronically or on paper. Rules on the right of appeal, the obligation to provide guidance, the speed of handling a case, investigation, equality and proportionality - to name but a few principles of administrative procedure, thus applied to the administration of a case irrespective of whether this was done electronically or on paper, and therefore did not need to be examined from the particular viewpoint of the electronic dissemination of information. Accordingly, the electronic dissemination of information did not call for separate rules, except insofar as they were required by the distinctive nature of this technology compared with traditional forms of communication.

The committee's report[1] stated that given that new technology attempted to serve the same interests as traditional methods had done hitherto, its examination of the legal questions concerning the electronic handling of cases concentrated on three main areas. These were:

1 *Skýrsla nefndar um rafræna stjórnsýslu*, 12, *cf*. "http://forsaetisraduneyti.is/utgefid-efni/nr/1325".

- To establish which rules obstructed in some way the use of electronic dissemination of information in administrative procedures.
- To identify the arguments fundamental to these rules and the needs they were supposed to fulfil.
- To examine whether the electronic dissemination of information could fulfil those needs, and if so, which prior conditions needed to be met.

The committee's findings were that the distinctive characteristics of the electronic dissemination of information required a number of rules to be set down inorder for it to be deemed as equally valid as traditional methods and to fulfil the material requirements – that is, . the arguments or needs underlying the formal requirements – generally made in relation to the handling of administrative cases. On the basis of the committee's proposals the Prime Minister laid a Bill before Parliament amending the Administrative Procedures Act and recommending the inclusion of a new chapter on the electronic handling of administrative cases. As mentioned earlier, this Bill became Act no. 51/2003.

The rules contained in Chapter IX of the Administrative Procedures Act do not, therefore, add new material rules to procedural law, but merely aim to adapt the formal requirements to meet changing methodologies and circumstances. These rules will be discussed in more detail in sections 6-14 below.

5 Main Principles upon which Chapter IX of the Administrative Procedures Act is Based

5.1 Introduction

The general remarks accompanying the bill amending the Administrative Procedures Act outline the main principles on which the provisions on electronic administration in Chapter IX of Act no. 37/1993 are based. The following are the five most important principles that are significant in interpreting the provisions of the Act.

5.2 The Equal Validity Approach

The Act is based upon making the same material requirements towards the handling of an administrative case irrespective of whether it employs traditional or electronic procedures. Consequently, the Act only contains such special rules on the electronic handling of administrative cases as are necessitated by the distinctive properties of IT. These special rules aim to make IT as equally valid as the methods that have been customary in administrative operations, insofar as this technology can serve the same interests. Thus the Act contains special rules with reference to various formal requirements made by laws in force, administrative actions and customs, for acts to be written and signed. These rules

aim to make electronic acts as equally valid as written acts, and electronic signatures as valid as traditional handwritten signatures, on fulfilment of specific conditions. In effect this removes the legal obstacles that generally might impede the electronic management of administrative cases.

If a law requires other formal conditions than those covered by the equal validity rules of Chapter IX of the Administrative Procedures Act, the result could be that information cannot be disseminated electronically in dealing with the case covered by that law. Such legal provisions will need to be reviewed separately if grounds are seen for allowing the electronic dissemination of information in the areas that they cover.

5.3 Technical Impartiality

The provisions of Chapter IX of the Administrative Procedures Act are based upon rules on the electronic handling of administrative cases that are as technically impartial as possible, and sufficiently flexible to remain unaltered notwithstanding foreseeable developments in IT.

5.4 Authorisation but not Obligation to Conduct Administrative Cases Electronically

Article 35 of the Administrative Procedures Act enables authorities to take advantage of IT in dealing with administrative cases. The provisions of Chapter IX do not oblige authorities to adopt such procedures in all areas, whatever may happen later. Authorities are generally deemed to be best qualified to judge whether (and if so, how) electronic administrative procedures should be adopted in individual fields, according to the circumstances prevailing with general government policy. Thus electronic administration will foreseeably be introduced in those areas where the greatest gains in efficiency and administrative effectiveness are to be expected.

The electronic dissemination of information can be used in dealing with administrative cases to varying extents. An authority can provide for a case to be handled *partly* or *entirely* by electronic means. Thus the authority may allow applications to be submitted in electronic format, even if its decision (for example, a licence) is presented to the party concerned in writing on paper.

5.5 General Rules on Electronic Administration

Chapter IX of the Administrative Procedures Act contains what can be considered to be general provisions on the electronic handling of administrative cases. Nonetheless, more stringent or lenient requirements may be made for electronic administration in specific areas, if deemed necessary. It should be underlined, however, that authorisation in law is needed for these general administrative principles to be superseded.

5.6 Civil Equality and Access to the Administration

The provisions of Chapter IX of the Administrative Procedures Act are based upon the guiding principle of civil equality in the use of IT. This entails that the legal provisions do not authorise authorities to deal with cases exclusively by electronic means, should they decide to introduce such a service, since it follows from the principle of proportionality, at least under present circumstances, that the public may present applications to authorities irrespective of whether or not they have the opportunity to do so electronically.

6 Scope of the Provisions of Chapter IX of the Administrative Procedures Act on Electronic Administration

The provisions of Chapter IX of the Administrative Procedures Act on electronic administration have the same scope as other Chapters of the Act. Thus the law applies in the handling of cases aimed at delivering an administrative decision. It follows from the general scope of the Administrative Procedures Act that the provisions of the Chapter apply solely to government authorities and not to parliament, institutions under its auspices, or courts of law.

The remarks accompanying the Bill incorporating Chapter IX of the Administrative Procedures Act point out that "information technology" is a broad concept embracing any kind of dissemination of information using electronic signals. This sweeping definition therefore includes, for example, fax, telegraphic and telephonic transmissions. Although these media thereby fall within the special rules in the Chapter, it follows from the provisions in it that the dissemination of information by computer is of prime significance, given that other media can rarely fulfil the requirements made in other Articles of the Bill.[2]

7 Authorisation for Electronic Handling of a Case

According to Article 35, paragraph 1, item 1 of the Administrative Procedures Act, the authority shall decide whether to offer the option of applying the electronic dissemination of information in the handling of a case. The appended remarks on the Article state that it was not considered practicable to oblige authorities to offer the public such a service, even though this is the aim wherever it may prove cost-efficient. In this context it should be pointed out that various technical and organisational complications need to be considered before electronic administration is introduced. It is therefore at the authorities' discretion to assess where they wish to offer electronic administration. On the other hand, the provision does not entail an authorisation that administrative cases may be dealt with solely by electronic means. It follows from the principle of proportionality, at least under present circumstances, that the public must be

2 Parliamentary Record: Alþt. 2002-2003, Section A, p. 1608-1609.

able to present applications to the authorities irrespective of whether or not they have the opportunity to do so by electronic means.

When an authority decides to offer the option of electronic administration, it is obliged to ensure that the party to the case is aware from the start about the hardware and software requirements that it must fulfil in order for it to be conducted electronically, and shall draw the party's attention to these requirements as the circumstances require, cf. Article 35, paragraph 1, item 2 of the Act. This entails that the authority shall decide which equipment is necessary for the party to transact electronically so that the case may be conducted in part or in whole by electronic means. In general, the requirements made by the authority in this respect will be determined by the hardware and software that it uses itself or has installed in the service of electronic administration.

Although authorities will decide for themselves on the requirements to be met in this respect, they are obliged to make these known at the beginning of a case and make them accessible to parties requesting a case to be handled electronically. For example, if notifications and other documents from the authority are created using specific software, information to this effect ought to be made known from the outset, so that a party to the case can decide whether it has the capability to receive electronic documents from the authority. These requirements should be accessible to the party – for example, stated on the authority's website where specifications on electronic administration are found. Such requirements would often constitute part of the authority's guidance concerning electronic handling of the case - for example, where an electronic form is to be completed using software that is custom-designed for a specific procedure.

Since parties to a case should be aware of the hardware and software requirements that need to be met for the case to be handled by electronic means, they are responsible for fulfilling such conditions. This is underlined in Article 39, paragraph 1, item 2 of the Act, which states that a party to a case is responsible for its hardware and software meeting the requirements that are made and are necessary for the party to be acquaint itself with the content of an administrative decision or other documents that the authority sends to it in electronic format.

Article 35, paragraph 1, item 3 of the Act states that authorities shall choose their hardware and software for use in electronic administration so that as many people as possible can take advantage of this option. Authorities are therefore obliged to strive to ensure that the solutions offered are technically impartial, where this can be arranged. Based upon the principle of proportionality, this provision entails that authorities should avoid electronic administration arrangements that require the public to incur the expense of buying new hardware and software or upgrading existing facilities. Thus authorities should always arrange electronic administration in such a way that the necessary software can be acquired without undue expense.

Article 35, paragraph 3 prescribes that an authority may decide the requirements that documents, which it receives electronically, need to fulfil. This provision is important as regards both the efficiency of electronic administration and security considerations. Authorities may therefore decide that applications

should be submitted in a specific format and to a specific location – for example, an agency's separate electronic handling centre.

Article 35, paragraph 3, item 2 of the Act stipulates that an authority may expressly provide for documents to be submitted to it using special electronic forms, that is, electronic documents in a standardised form for the party to complete. If an application fails to meet these requirements, the authority should offer guidance and request that the party should complete the form correctly, or otherwise provide the necessary information or meet such other conditions that the authority has laid down in accordance with this item of the Act. If a party fails to act upon a reminder to this effect from the authority, it depends upon the legal sanction on which the decision is based whether the authority should reject the case or resolve it on the basis of the documents that have been acquired and that can be acquired. An electronic application that is not submitted to the correct location within the administration must be forwarded in accordance with the provisions of Article 7, paragraph 2 of the Administrative Procedures Act. This provision also allows an authority to make requirements aimed at preventing the submission of documents that may contain viruses or in other respects pose a threat to the security of its computer system.

An authority that expressly provides for documents to be submitted on special electronic forms is obliged to provide standardised guidance on completing them and the requirements that it makes, cf. Article 3, paragraph 3, item 3 of the Act. Since employees of the authority generally do not communicate directly with parties to an electronic administration case, they do not have the same grounds as otherwise for assessing which initiative the party requires. For this reason, it was felt necessary to state expressly the authorities' duty to provide standardised guidance on the completion of electronic forms.

An authority that decides to offer the option of electronic administration of a case is obliged to handle it by electronic means if the party so requests. The same applies if the party's application suggests a request for electronic handling. In general this should be seen as applying when a party, on its own initiative, has used the electronic facilities that an authority has advertised on its website as being available for communicating with it. If the party contacts an authority electronically, but nonetheless requests a reply by traditional means, the authority is obliged to comply, unless the provisions of separate legislation specify otherwise.

8 Legal Provision Requiring Written Documents in the Handling and Resolution of a Case

In many areas of Icelandic law, express provision is made for written documents. Current rules often invite the interpretation that electronic documents fulfil their conditions of being considered *written*. Although there are grounds for such an interpretation, it is clear that in particular cases substantial doubt may exist as to whether such a view is admissible. Accordingly, it was felt desirable to amend the Act so that electronic documents should be considered as equally valid as written ones within the administration, provided that they

fulfilled minimum requirements for being accessible, preservable and transferable.

Article 36 of the Administrative Procedures Act stipulates that when laws in force, administrative acts or customs expressly provide that documents sent to a party to a case or an authority shall be in writing, those in electronic form shall be considered to fulfil that provision if they are technically accessible to the recipient, who can thereby acquaint himself, or herself, with their content, preserve them and forward them. The purpose of this provision is that electronic documents shall have the same status as written documents once certain conditions are met, so that it embodies a rule of the same kind as Article 8, paragraph 1 of Act no. 30/2002, on Electronic Commerce and other Electronic Services. These conditions should ensure that electronic documents serve all the same interests as written documents with respect, for example, to verification, reproduction and storage.

The remarks on Article 36 accompanying the Bill on the Administrative Procedures Act[3] state that in order for an electronic document to be considered as equally valid as a written document, it needs, firstly, to be technically accessible using the hardware and software specified in the terms set forth by the authority, cf. Article 35 of the Act. This emphasises that the authority is obliged to notify parties in advance of the requirements that their hardware and software need to fulfil to enable receipt of documents, and that parties to a case are responsible for having adequate equipment in this respect. Documents that would be generally technically accessible would thus also be considered to be written in the sense of this provision, even though a party could not acquaint itself with their content owing to inadequate facilities. However, documents that were inaccessible even if normal requirements for resources were met would not fulfil the condition of being considered accessible. Documents that were inaccessible without acquiring special hardware or software would therefore fail to meet this condition. The same would apply to documents that needed to be converted with expert assistance or using unconventional facilities.

Secondly, documents must be preservable in a comparable manner to the preservation of paper documents. Documents submitted telephonically, for example, can only be preserved by recordings, and would not be considered preservable in this sense. One purpose served by this condition is to admit an electronic document as permanent verification of a declaration or act in a comparable fashion to a paper document.

The third condition for an electronic document to fulfil a legal requirement of existing in writing is the possibility of presenting it later. In other words, it must be possible to reproduce a document and distribute it in a similar fashion to paper documents. This condition attempts to ensure that an electronic document can perform the same function as a written document in various respects; for example, if there is a need to submit it to other authorities or courts of law, or grant access to it on the basis of the Information Act.

3 *Cf.* Alþt. 2002-2003, Section A, 1611.

9 Provision Requiring an Original or a Copy

Electronic documents can hardly be considered to exist in original form in the conventional sense of the term. Computer-readable documents are in effect a specific presentation and at the same time a copy of electronic information which is compiled from patterns (electrically charged and uncharged) and can be described in binary notation (0 and 1). The information concealed in these patterns is only accessible by using suitable hardware and software. It should be borne in mind that the same original digital data may be presented differently when read by different hardware and software systems. Thus the concepts of 'original' and 'copy' are broadly inappropriate for electronic documents. Electronic documents, as they appear on a computer display or by other means, can always be described as a copy of digital information.

Legal requirements for an original document serve the purpose of ensuring that it is unchanged. Thus it is natural to regard an electronic document as fulfilling this provision, if it can be ensured that the document is unchanged from its completion, which is primarily a technical question.

Article 37, paragraph 1 of the Administrative Procedures Act stipulates that when laws in force, administrative acts or customs expressly provide that a document shall be in its original form, electronic documents shall be considered to fulfil this provision if it is ensured that they are unchanged. The remarks on this Article of the Bill[4] state that the technology to be used must be taken into account in assessing whether the condition of this provision, that an electronic document is unchanged since its completion, is met. Electronic signatures are a method particularly plausible for examining whether a document has changed since being electronically signed.[5]

Article 37, paragraph 1, item 2 of the Administrative Procedures Act makes a proviso that electronic documents cannot be regarded as a commercial or other type of deed or other deed where financial rights are vested in the holding of it. Specific legislation has been passed on the electronic form of such deeds, namely Act no. 131/1997, on the Electronic Registration of the Title to Securities.

Rules on *copies* serve the purpose of making documents available in more than one identical version. Since electronic documents are easy to copy, it is pointless to require them to be submitted to or by authorities in more than one

4 *Cf.* Alþt. 2002-2003, Section A, 1612.

5 Act no. 28/2001 on Electronic Signatures addresses such signatures. An electronic signature is the encryption of digital information with a private cryptographic key. The identity of the owner of a private key and the integrity of the message can be established by using a corresponding public cryptographic key and a certificate from a signature certification provider stating the originator of the keys. The digital information encrypted with a private key to create the signature is termed the message digest value. The message digest value (X) is yielded by encrypting the documents to be signed and sent, using a one-way algorithm. When the documents and the electronic signature are received, the process is repeated using the same algorithm as the sender, to yield the message digest value Y which is compared with that of the sender. If message digest value X equals Y, the documents have not been tampered with. If X is not equal to Y, the documents have been changed, wilfully or accidentally; in either case, the message digest value has changed.

copy. Article 37, paragraph 2 of the Administrative Procedures Act thus stipulates that when laws in force, administrative acts or customs expressly provide that documents shall be presented in more than one copy, documents in electronic format shall be considered to fulfil this provision.

10 Legal Provision Requiring a Signature and Witnessing of it

Various administrative rules expressly provide for, or vest specific legal effects in, the signature of a deed. There are various arguments for a legal provision requiring a signature. Generally, however, the primary intent is to ensure the signatory's personal confirmation of specific matter contained in the signed document, for example, a declaration of intent, a decision, and so on. Thus a signature serves the principal aim of verifying that a specific person has confirmed something that is stated in what is signed. The signed article is normally a text containing certain information. Signatures also serve to confirm that other signatures are correct, and possibly other details, for example, such things as financial independence and the date. It should be remembered that signatures may also possess various other significances than verifying personal confirmation. One example is the use of a signature to ensure that a signatory is more aware of an obligation undertaken with a declaration to that effect.

In Iceland, electronic confirmation has for the most part been in the form of pin numbers or passwords, but it is questionable whether such confirmation should be considered to be a proper electronic signature. Sophisticated electronic signatures, based upon Public Key encryption, have not yet become widespread. Such electronic signatures are created by certification service providers who assign cryptographic keys to users and generally also issue authentication certificates to verify that the signature originates from a specific party. These can unquestionably have the same value in verification as written signatures and appear to be able to replace them entirely.

Act no. 28/2001 on Digital Signatures was passed following Decision no. 66/2000 by the joint EEA Committee, to append to Protocol XI of the EEA Agreement Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. The Act provides for the legal effect of electronic signatures, activities of certification service providers, certification with electronic signatures, supervision of certification service providers and their responsibilities towards the public. The main principle of the Act, stated in Article 4, is that in the event of a signature being a condition for legal effect pursuant to legislation, administrative requirements or for other reasons, a qualified electronic signature shall in all cases fulfil such requirements. Under Article 3, paragraph 7 of the Directive, Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. The rule proposed in the Bill of Amendment, however, assumes that the same requirements will be made in relation to electronic signatures in the handling of administrative cases, as in civil transactions in law in accordance with the legislative policy laid down in Act no. 28/2001.

Article 38, paragraph 1 of the Administrative Procedures Act prescribes that when laws in force, administrative acts or customs expressly provide for documents from a party or an authority to be signed, the authority may decide that an electronic signature shall replace a handwritten one, provided that it ensures in a comparable manner the personal confirmation of the party from whom the documents originate. In order for this to be allowed, an electronic signature must ensure, in a comparable fashion to a handwritten one, the personal confirmation of the party from whom the signature gives the impression of originating. Thus the technical properties of a specific electronic signature, in particular, determine whether these conditions have been deemed to have been fulfilled. A qualified electronic signature in the sense of the Act on Electronic Signatures, however, is automatically regarded as fulfilling the condition. Materially, this is the same rule as found in Article 4 of Act no. 28/2001, on Electronic Signatures. Other signatures may be sufficient on further decision of the authority, as pointed out above. This rule corresponds materially to Article 4 of the same Act, except that it rests with the authority to take a prior position towards the value of a signature in this respect. The concepts "electronic signature" and "qualified electronic signature" are used here in the same sense as in Act no. 28/2001, on Electronic Signatures.

Article 38, paragraph 2 of the Administrative Procedures Act affirms that an electronic signature fulfilling the conditions of paragraph 1, or a qualified signature, meets the legal requirement of being considered to be certificated in specific respects, if it is supported by a certificate confirming such details as are required to be certificated. Qualified electronic signatures must be certificated by a certification service provider, as specified in the Act on Electronic Signatures. Thus it is not deemed necessary for an electronic signature to be specially certificated by other parties, as is sometimes insisted on in the case of conventional signatures. A certificate for an electronic signature that, for example, also certificates the date and age of the signatory, would according to the law also fulfil a legal provision on the witnessing of the signature, the date and financial independence.

Article 38, paragraph 3 of the Administrative Procedures Act affirms that authorities may use confirmation other than electronic signatures; for example, passwords, in instances where the law does not specifically require a handwritten signature. Thus in effect the rule does not entail a change from current law, but underlines that electronic confirmation may be used when there is no legal obligation to sign documents by hand. Whether this would be considered to be right in a given case depends upon both the technical assessment of the security of passwords and the nature of the case in point.

11 When is an Electronic Application Considered to have Reached an Authority?

Article 39, paragraph 2 of the Administrative Procedures Act prescribes that applications or other documents are considered to have reached an authority when it has the opportunity of acquainting itself with their contents. It is stated

that an authority shall, on its own initiative, confirm that it has received documents, where possible.

Major interests often hinge on documents reaching authorities before a given deadline. Parties to cases should therefore normally be able to obtain confirmation that documents were sent to an authority at a certain time and successfully delivered. Nevertheless, a security precaution was made law with Article 39, paragraph 2 of the Administrative Procedures Act, whereby authorities shall confirm receipt of electronic documents so that a party to a case shall know that its application has been received at a certain time, and where appropriate within a given deadline. Since it may be assumed that receipt can often be automatically confirmed, there is no reason to presume that this rule will prove an excessive burden on the authorities.

12 Announcement of an Administrative Decision

The time limits for the handling of administrative cases depend in many instances on when the party to the case has received notification from the authorities. Article 27 of the Administrative Procedures Act, for example, prescribes that a complaint shall be lodged within three months of the notification to a party of an administrative decision, unless otherwise provided for by the law, while according to Article 20, paragraph 1 of the same Act, a decision shall be binding upon notification to a party.

A notification is generally considered to have reached a party when that party has had the opportunity of acquainting itself with its contents. Notification of an administrative decision would therefore be considered to have reached a party when a letter containing such notification has been delivered to the party's household or mailbox. Verbal notifications of decisions in the presence of a party are deemed to have reached it immediately. The same applies to documents that a party sends or has delivered to an authority. The sending and reception of notifications in electronic form is subject to the same principles as other notifications. In general, electronic documents would therefore be deemed to have reached persons when they have had the opportunity of acquainting themselves with their contents. For example, if an email was accessible to a party on its server, it would be deemed to have reached it in the above sense.

In accordance with the above viewpoints, Article 39, paragraph 1, item 1 of the Administrative Procedures Act prescribes that a party has been notified of an administrative decision or other documents in electronic form when it has had the opportunity of acquainting itself with the contents. With this provision, the general administrative rule on notification is adapted to information technology, in accordance with which it proposes that electronic documents are deemed to have reached a party when it has had the opportunity of acquainting itself with the contents. For example, an email which is accessible to a party on its server would be deemed to have reached it in the above sense. If documents are not accessible to a party for technical reasons for which it cannot be considered responsible, and which prevent it from acquainting itself with the contents, they are not deemed to have reached that party. For that reason, authorities are

obliged to give a prior description of the requirements that the party's hardware and software need to meet so that the case can be handled electronically, and to make these requirements accessible to the party when the case is opened, as discussed more fully in Section 7. Article 39, paragraph 1, item 2 of the Administrative Procedures Act states that a party to a case is responsible for its hardware and software fulfilling the requirements that are made, cf. Article 35, paragraph 1 of the Act, and that are necessary in order for the party to acquaint itself with the administrative decision or other documents sent by the authority in electronic format. In this context it should be emphasised that a party is not obliged to take part in the electronic handling of a case in accordance with the provisions of this Bill, and always retains the option for a case to be dealt with by conventional means.

13 Verifiable Transmission

Some laws expressly provide for documents to be sent by verifiable means such as registered mail. Information technology can clearly verify securely whether and when documents are deemed to have reached a party; among other things, devices for creating electronic signatures can serve this purpose. In light of this, Article 39, paragraph 3 of the Administrative Procedures Act prescribes that when laws in force, administrative acts or customs expressly provide that authorities shall present documents by verifiable means, such a provision is considered to be fulfilled by the use of electronic equipment that confirms that the documents have reached the party concerned. This provision avoids the need to print documents and deliver them by conventional means when electronic procedures are available.

14 Preservation of Electronic Documents

Under Article 22, paragraph 1 of the Information Act, no. 50/1996, Government authorities are obliged to register the cases that they handle in a systematic manner, and to preserve the materials relating to such cases so that they are accessible. Preservation of documents is subject to the provisions of Act no. 66/1985, on the National Archive of Iceland, Article 6, which states that documents, which it is mandatory to store, shall normally be presented to the archive no later than when they are thirty years old.

Strong public interests hinge upon being able to take the authenticity of public documents for granted, and the same applies to electronic documents. Accordingly, Article 40 of the Administrative Procedures Act prescribes that an authority shall preserve electronic documents in such a way that their substance and origin can be subsequently verified by accessible means.

Electronic signatures are useful for ascertaining the authenticity of electronic documents on their receipt. Since certification of electronic signatures is only assumed to be valid for a limited time, the authorities must preserve electronic documents in such a way that their authenticity can be verified later, even if the

certification of electronic signatures is no longer valid and the signatures to the documents have expired. If public document storage systems are secure, it may be assumed that documents submitted to an authority at a certain time are unchanged. If the authenticity of the document has been ascertained on its receipt or storage, and if such scrutiny can later be invoked, it is not a critical issue if the certification of an electronic document is no longer present.

It should be borne in mind that electronic documents are normally only accessible with the appropriate hardware and software. Storage of electronic documents should therefore ensure either that such hardware and software are at hand or that the documents are upgraded as these evolve. From a technical perspective these should not be insurmountable problems. On the other hand, it is important for both the government authorities and the National Archive to resolve them at the earliest possible opportunity. Before this is established, it is not justifiable to recommend the large-scale adoption of e-government. By the same token, it is important to seek partial or complete solutions to such problems at central level for the government administration, since it does not seem prudent, nor efficient, to expect each respective authority to "reinvent the wheel" in this respect.

15 The Security of Electronic Administration

According to Article 11, paragraph 1 of Act no. 77/2000, on the Protection and Processing of Personal Data, cf. Article 5 of Act no. 90/2001, the controller shall implement appropriate technical and organisational measures to protect personal data against unlawful destruction, against accidental loss or alteration and against unauthorised access. A controller is the party that determines the purposes of the processing of personal data, the equipment that is used, the method of the processing and other usage of the data, cf. Article 2, item 4 of the same Act. In the case of government authorities, the controller in this sense is generally the head of the agency in question or, where appropriate, the government minister.

Article 11, paragraph 2 of Act no. 77/2000, with subsequent amendments, states that having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. According to Article 11, paragraph 5 of the same Act, the controller shall document how he produces a security policy, conducts a risk analysis and decides on security measures to be implemented. Article 12 of Act no. 77/2000 prescribes that the controller shall conduct internal audits on the processing of personal information to ensure that they are processed in accordance with prevailing laws and regulations and the security measures that are to be implemented. Rules no. 299/2001, on the security of personal data, prescribe in more detail the arrangements for preparing a system of security procedures to ensure the protection of personal data.

According to Article 11, paragraph 4 of Act no. 77/2000, the controller is responsible for risk analysis being reviewed routinely and security measures upgraded to the extent necessary to fulfil the requirements of that Article.

Privacy is not the only interest that calls for adequate security to be ensured in the processing of information by the public administration. The public interest demands effective measures to prevent the operations of the government authorities from being paralysed by sabotage or other setbacks, accidentally or incidentally. For this reason, in implementing electronic administration, the authorities need to maintain continually anti-virus protection and other necessary security measures to defend the system against such setbacks.

It is the responsibility of the controller to implement all appropriate technical and organisational measures *before* an authority offers the public the option of using electronic dissemination of information in dealing with administrative cases.

Although the Administrative Procedures Act does not include any specific security rules, on the basis of those described above it can be said that Article 40 of the Act entails a general provision that appropriate security measures should be taken at any time in connection with the preservation of documents.

Supplementary provisions
Chapter IX of Act no. 37/1993, on Administrative Procedures, cf. Act no. 51/2003.
Electronic administration

Article 35
Authorisation for electronic handling of a case

An authority shall decide whether to offer the option of using electronic dissemination of information in the handling of a case. The requirements that a party's hardware and software requirements must fulfil in order for a case to be conducted electronically shall be accessible to it at the start of a case and the authority shall draw the party's attention to these requirements as the circumstances require. These requirements shall be set with the aim that the equipment of as many parties as possible can be used.

An authority that decides to exercise the authorisation under paragraph 1 shall use electronic dissemination of information in handling a case if a party so requests. The same applies when a party, on its own initiative, has used the electronic facilities that an authority has advertised on its website as being available for such communication.

An authority may decide the requirements that documents, which it receives electronically, need to fulfil. An authority may inter alia expressly provide for documents to be submitted to it using special electronic forms. The authority shall then provide standardised guidance on completing the form and the requirements that it makes.

Article 36
Formal requirements

When a law in force, a general administrative act or custom provides that documents sent to a party to a case or an authority shall be in writing, those in electronic form shall be considered to fulfil this provision if they are technically accessible to the recipient, who can thereby acquaint himself with their content, preserve them and forward them.

Article 37

Originals and copies

When laws in force, administrative acts or customs expressly provide that a document shall be in its original form, electronic documents shall be considered to fulfil this provision if it is ensured that they are unchanged. This does not apply, however, to a commercial or other type of deed or other deed where financial rights are vested in the holding of it.

When laws in force, administrative acts or customs expressly provide that documents shall be presented in more than one copy, documents in electronic format shall be considered to fulfil this provision.

Article 38
Electronic signatures

When laws in force, administrative acts or customs expressly provide for documents from a party or an authority to be signed, the authority may decide that an electronic signature shall replace a handwritten one, provided that it ensures in a comparable manner the personal confirmation of the party from whom the documents originate. A qualified electronic signature according to the Act on Electronic Signatures shall in all cases be consider to fulfil the legal provision on signatures.

When laws in force, administrative acts or customs expressly provide for a document or particular details of it to be certificated, such a provision is considered to be fulfilled with an electronic signature according to paragraph 1, confirming such details as are required to be certificated.

When laws in force, administrative acts or customs do not expressly provide for documents from a party or an authority to be signed, an authority may decide that other methods than electronic signatures may be used to confirm electronic documents.

Article 39
Electronic handling of a case

A party is considered to have been notified of an administrative decision or other documents in electronic form when it has the opportunity to acquaint itself with the contents. A party to a case is responsible for its hardware and software fulfilling the requirements that are made, cf. Article 35, paragraph 1, and that are necessary in order for the party to acquaint itself with the administrative decision or other documents sent by the authority in electronic format.

Applications or other documents are considered to have reached an authority when it has the opportunity of acquainting itself with their contents. An authority shall, on its own initiative, confirm that it has received documents, where possible.

When laws in force, administrative acts or customs expressly provide that authorities shall present documents by verifiable means, such a provision is considered to be fulfilled by the use of electronic equipment that confirms that the documents have reached the party.

Article 40

Preservation of electronic documents

An authority shall preserve electronic documents in such a way that their substance and origin can be subsequently verified by accessible means.