



Abenhed

Guide on How to Use Mandatory Open Standards for Software in the Public Sector



National IT and Telecom Agency

Ministry of Science
Technology and Innovation



Use of Mandatory Open Standards for
Software in the Public Sector

Published by:
National IT and Telecom Agency

National IT and Telecom Agency
Holsteinsgade 63
DK-2100 Copenhagen Ø

Telephone: +45 33 92 97 00
Fax: +45 33 32 35 01

This publication may be obtained free of
charge, subject to availability of stock,
from:

National IT and Telecom Agency

The publication may also be downloaded
from the Agency's website:

<http://www.itst.dk>

ISBN (Internet): 87-91702-96-8

>

Use of Mandatory Open Standards for Software in the Public Sector

Contents

>

Mandatory open standards	6
Government decision and agreement on the use of open standards for software in the public sector	6
Mandatory open standards	7
Use of mandatory open standards	8
Use of mandatory open standards	9
Which standards are relevant?	9
Authority's own development	10
Procurement and tenders	10
Justification for applying exemption rules	11
Application of exemption rules must be published	12
Sets of mandatory open standards	13
Standards for data exchange between public authorities (OIOXML)	14
Main principle of OIOXML	14
Primary scope of OIOXML	14
Mandatory open OIOXML standards	14
Requirements for use of OIOXML	14
Standards for electronic file and document handling (FESD)	16
Main principle of FESD standards	16
Primary scope of FESD standards	16
Mandatory open FESD standards	16
Requirements for use of FESD standards	16
Maintaining the requirement for use of FESD standards	17
Standards for electronic procurement in the public sector (OIOUBL)	18
Main principle of electronic procurement	18
Primary scope of OIOUBL	18
Mandatory open OIOUBL standards	18
Requirements for use of OIOUBL	19
Standards for digital signatures	20
Main principle of OCES digital signatures	20
Primary scope of OCES digital signatures	20
Mandatory open OCES standards	20
Requirements for use of OCES digital signatures	21
Maintaining the requirement for use of OCES digital signatures	21
Standards for public websites and accessibility	22
Main principle of public websites	22
Primary scope of standards for public websites	22
Mandatory open standards for public websites	22
Requirements for use of public websites	22

Standards for IT security (DS484)	24
Main principle of information security	24
Primary scope of DS484	24
Only applicable to the government sector	24
Mandatory open standards for information security	25
Requirements for use of DS484	25
Standards for document exchange (ODF/OOXML)	26
Main principle of document standards	26
Primary scope of document standards	26
Mandatory open document standards	26
Requirements for use of document standards	26
Maintaining the requirement for use of document standards	26
OIO catalogue	28
International anchoring of the OIO catalogue	28
Adjustments of the OIO catalogue	28
Structure of the OIO catalogue	29
New mandatory open standards	30

Mandatory open standards



From 1 January 2008, it will be mandatory for public authorities in Denmark to use a number of open standards for future procurement of software and IT solutions.

This means that Danish public authorities have to make sure that their future IT solutions are based on, or support, these mandatory open standards if the standards are relevant to the IT solution. All the mandatory open standards are subject to the condition that the individual authority, in case of additional expenses or for reasons of IT security in the authority concerned, may omit to use such standards.

The use of mandatory open standards does not imply any exclusion of standards other than the mandatory open standards. So IT solutions are still allowed to employ standards other than mandatory open ones as long as the solutions also support the use of relevant mandatory open standards.

There is no requirement that specific software types or products should be used, and there is no requirement that the formats concerned should be used as the internal software format.

Public authorities mean local and regional administrations, government departments, agencies and directorates.

Mandatory open standards mean selected and named standards found suitable for use in the public sector.

This Guide is based on an agreement between the Danish Government and the local and regional administrations in Denmark, as represented by Local Government Denmark and Danish Regions, see below.

Government decision and agreement on the use of open standards for software in the public sector

On 2 June 2006, the Danish parliament (the Folketing) unanimously adopted Parliamentary Resolution B103 on the use of open standards for software in the public sector. The Resolution instructs the Government to ensure that the public sector's use of information technology, including the use of software, should be based on open standards. A majority of the political parties have made it a condition that the use of open mandatory standards must not involve increased costs to the public sector.

On 11 August 2006, the report "Measures to Promote Interoperability via Common Open Standards" was published. The report had been commissioned by the Ministry of Science, Technology and Innovation, the Ministry of Finance, Local Government Denmark and Danish Regions. The report provided a common public basis on how the use of mandatory open standards might be implemented. This included a suggestion that such use should be implemented via a Government decision and an agreement with local and regional administrations.

In February 2007, the National IT and Telecom Agency held a consultation on the report "Use of Open Standards for Software in the Public Sector". This report recommends that seven software standards should be made mandatory with effect from 1 January 2008.

The consultation responses were mainly positive, and subsequently the Minister for Science, Technology and Innovation achieved political support for a timescale for implementing the use of mandatory open standards for software in the public sector.

Mandatory open standards

The introduction of open standards is intended, without involving increased costs to the public sector, to promote a competitive market for software and contribute to public IT systems being able to exchange information across the sector irrespective of the choice of software.

For each potential set of mandatory open standards, an economic impact assessment is to be carried out. The assessment will ensure that the introduction of a particular standard is expedient in socioeconomic terms.

That a standard is open implies that:

- the standard must be fully documented and publicly available,
- the standard must be freely implementable without any economic, political or legal constraints on its implementation and use, now or in future, and
- the standard must be standardised and maintained in an open forum via an open process (standards organisation).

The first seven sets of mandatory open standards will enter into force from 1 January 2008. These are the following sets of standards:

- Standards for data exchange between public authorities (OIOXML)
- Standards for electronic record management (FESD)
- Standards for electronic procurement in the public sector (OIOUBL)
- Standards for digital signatures (OCES)
- Standards for public websites / homepages and accessibility
- Standards for IT security (DS484 - only for the government sector)
- Standards for document exchange (ODF/OOXML)

As for standards for document exchange, there are currently two significant open standards for these formats in the market: ODF and OOXML. However, both standards are still relatively immature, and detailed experience of their use in practice is lacking. As a result, the economic impact of introducing them is difficult to estimate, being based on a large element of discretion. This fact is also realised in other European countries facing similar decisions.

Therefore, the following will be implemented:

- On 1 January 2008, all public authorities in Denmark must be able to receive word processing documents from citizens, businesses and other authorities in two formats: OOXML and ODF.
- With effect from 1 January 2008, OOXML and ODF will be mandatory standards for public authorities. IT solutions procured after 1 January 2008 must support at least one of these open standards and be able to receive word processing documents in both formats, if necessary by using additional programs (plug-ins).

>

- Whether ODF and/or OOXML should be mandatory after 1 July 2009 will be decided following an assessment by an independent third party.

Use of mandatory open standards

The requirement to use mandatory open standards is only applicable to new IT solutions.

The use of mandatory open standards is subject to the condition that the individual authority, in case of additional expenses or other negative consequences, including IT security considerations in the relevant authority, may omit to use the mandatory standards.

Specific guidelines, including how an omission may be justified, are given in instructional guides prepared on the basis of the implementation of mandatory open standards.

Use of mandatory open standards

>

The true value of standards is realised only in their use. At the same time, it is important to avoid a situation in which specific authorities are forced to make inexpedient choices, expediting procurement and development in relation to administrative requirements, or in which they give up establishing an IT solution because it is too expensive or complicated. For this reason, there are a number of exemptions from the requirement for using mandatory open standards.

From 1 January 2008, all new development in the public sector is expected to employ mandatory open standards as a basic element.

This means that authorities launching tenders and development projects in areas where mandatory open standards have been defined should include these as part of the project basis.

New solutions mean new procurement and new development, also including further development and upgrading of software, unless this forms part of an agreement already concluded.

In connection with tenders and development projects, authorities may exempt themselves from the rules on using mandatory open standards if this means that the authority is compelled to adopt a solution which:

- > is significantly more expensive compared to using other standards,
- > degrades the security level critically compared to using other standards,
- > involves a significant reduction in functional performance which is a direct result of the solution being based on mandatory open standards,
- > increases the implementation time markedly,
- > is in conflict with standards applicable within specific areas as a result of international commitments.

In case one or more of the points above are in evidence, the relevant authority may choose to depart from specific mandatory open standards for the solution concerned.

If it is found necessary to depart from the requirement, this will call for an *explanation*. This means that the authority in question has to give an explanation describing the specific circumstances of the situation that lie behind a departure from the requirement for compliance with the mandatory set of open standards.

In combination, the requirements and the conditions justifying a departure from these constitute a *comply or explain* model.

Which standards are relevant?

The individual authority should start assessing the question of using mandatory standards in connection with the initial analysis phase of a given IT project. The

assessment consists in identifying which of the mandatory open standards are relevant to the area covered by the system solution.

Authority's own development

Where project management competency is chiefly held by the authority itself, assessment of any negative consequences of using mandatory open standards should be completed before the project launch is finally approved.

Procurement and tenders

For procurement with or without a tendering process, such assessment should be included in the specification of requirements or as an appendix to this, and at the same time the authority should clearly indicate its expectation that the solution described by the supplier be based on a set of mandatory open standards in case it is relevant to use these within the scope of the solution to be provided.

When such requirements for the use of standards are listed, the supplier should be made aware of the background, i.e. the main principles underlying *comply or explain*. Similarly, the supplier should be informed of what standards are mandatory at any given time. Finally, the supplier should be made aware that the requirement may be departed from with reference to the current exemption rules. In case one or more of the reasons for departing are in evidence, and the supplier estimates that this should have an influence on the description of the solution, a specific justification for this should be prepared.

Thus the authority will be presented with a solution from the supplier addressing the question of whether it is relevant to use open mandatory standards in a given context, and, if so, whether these can be complied with or will fall within the exemption rules. In case the mandatory standard is used, this should be stated by the supplier. In case an exemption is made from such use, the specific circumstances and documentation underlying this should be stated.

How contracting authorities may include mandatory open standards in their tender documents

To ensure that contracting authorities include mandatory open standards when procuring IT solutions, it is proposed that tender documents should be drafted in the following way:

1. Allow the tenderer to submit alternative tenders if the tenderer estimates that it will not be expedient for the contracting authority to make use of the mandatory open standards in a specific context. This will enable the tenderers to submit two types of tender:
 - a tender based on/supporting mandatory open standards
 - a tender not based on/supporting mandatory open standards
2. The option of submitting alternative tenders should be stated in the contract notice. It is a requirement that contracts should be awarded on the basis of the award criterion "the most economically advantageous tender".
3. List requirements for the IT solution in the tender documents.

4. Specify which of these requirements are minimum requirements, i.e. requirements to be met by all tenders in order to comply with the conditions. These minimum requirements may address security, timescales and functionalities. International commitments to be complied with by the IT solution should also be included as minimum requirements.

When the contracting authority receives tenders, the authority may choose the most economically advantageous tender both among the tenders that fulfil all requirements of the tender documents and the tenders that have proposed alternative solutions.

It will also be part of this choice to assess any negative consequences that may result from choosing an IT solution based on/supporting mandatory open standards. These negative consequences are examined in more detail below.

Justification for applying exemption rules

A number of criteria have been listed determining when an authority may be exempted from the rules of applying mandatory open standards in a specific area. In these cases a detailed justification should be given of the need for such exemption.

Irrespective of whether the statement is prepared by the public authority, the private supplier or on a joint basis, the following information should preferably be included in the justification:

Increased development costs:

- > Estimated additional costs, both the actual figure and in proportion to the total acquisition cost.
- > State any negative consequences to other authorities arising because the solution does not use mandatory standards.

Degraded security level:

- > State why the security level is believed to be significantly degraded.

Functional deterioration:

- > State the reasons why a functional deterioration is expected as a result of mandatory open standards being used, including whether this is due to one or more of the following factors:
 - Lack of integration capability.
 - Conflict with standards already in use which cannot be departed from.

>

Significant delay:

- > Assessment of how much the project will be delayed, and any related consequences.

Conflict with current sector standards:

- > If the exemption is justified with reference to conflicts with standards applicable in specific areas because of international commitments, then include a reference to the decision for the sector.

Application of exemption rules must be published

For new solutions where technical acquisition involves overall costs in excess of the EU tendering limit, the justifications for applying the exemption rules must be published. This can be made by:

- the authority submitting the justifications to the National IT and Telecom Agency when the contract is signed, the National IT and Telecom Agency arranging for publication,
- publishing the justifications on the authority's own website, or
- publishing the justifications in connection with financial reporting.

New solutions with overall costs below this limit should also employ mandatory open standards unless they fall within the exemption rules. However, these solutions are not subject to the requirement for publication of possible exemption rules. All the same, authorities are recommended to publish these as well.

The requirement for publication is not applicable to systems falling within the scope of the Security Circular issued by the Prime Minister's Office.

Sets of mandatory open standards

>

The potential value of a standard in terms of ensuring interoperability cannot be fully realised until it is actually applied, particularly when this is in association with other standards. Standards should therefore be regarded in an application context. An application context may be for example data exchange between systems, cross-sectoral user control, or citizens' access to public information via the Internet.

For each of such application contexts, there will typically be more than one relevant standard. It may therefore be said that a set of standards is associated with each context.

The Minister for Science, Technology and Innovation and the IT policy spokesmen of the Folketing have agreed on a timescale for implementing mandatory open standards under which seven sets of standards will be mandatory from 1 January 2008.

The seven sets of standards are:

- > Standards for data exchange between public authorities (OIOXML)
- > Standards for electronic record management (FESD)
- > Standards for electronic procurement in the public sector (OIOUBL)
- > Standards for digital signatures (OCES)
- > Standards for public websites / homepages and accessibility (HTML/XHTML, CSS and WCAG)
- > Standards for IT security (DS484)
- > Standards for document exchange (ODF/OOXML)

The following pages give a more detailed description of each individual set of standards.

Standards for data exchange between public authorities (OIOXML)

>

It is a basic condition for effective e-government that data exchange between systems should proceed as correctly and smoothly as possible - or, in other words, that interoperability between systems is possible.

For interoperability to be possible, it is necessary to standardise; and in Denmark a targeted effort has been made in the public sector since 2001 to enable such standardisation.

With a common set of standards for data exchange between the authorities' IT systems, the public sector may develop IT systems where information is defined in a uniform manner and can be reused across systems, thus allowing IT systems to be used for developing coherent services for citizens, businesses and other authorities across administrations and authorities.

Main principle of OIOXML

OIOXML is a language that provides the basis for establishing coherent data exchange between the IT system of public authorities, as OIOXML ensures that information can be exchanged in a uniform and intelligible way.

In concrete terms, OIOXML is a common description of the entire set of OIO data standards which, in combination, constitute the common public language for data exchange in the XML format.

Primary scope of OIOXML

The primary scope of OIOXML is the exchange of information between all public IT systems developed by the authorities covered by the agreement on using open standards for software in the public sector.

Mandatory open OIOXML standards

Mandatory open standards are:

- OIO data standards either adopted from international contributions or developed according to the current version of the common public set of rules known as OIO-NDR (= OIO Naming and Design Rules).
- XML Schema 1.0, maintained by W3C (www.w3.org/XML/Schema). The OIO-NDR is a profile (reduced version) of the XML Schema 1.0 recommendation, where constructions irrelevant to OIOXML etc. have been removed.
- Extensible Markup Language (XML) 1.0 (Third Edition), maintained by W3C (<http://www.w3.org/TR/2004/REC-xml-20040204>).

Requirements for use of OIOXML

To use OIOXML means that all data exchange follows specifications in existing OIO data standards, including new OIO data standards being developed as far as possible (following the principles of *comply or explain*) so as to meet any unfilled needs. The guidelines for application and development are as follows:

- For information already expressed in OIOXML, reuse existing OIO data standards in the manner described by OIO in relevant OIO guidelines.
- For information not yet covered by OIOXML, add new OIO data standards following the steps given below in order of priority:
 1. If there are international data standards covering the relevant need for exchange, adopt these as OIO data standards as indicated in relevant

>

OIO guidelines (if necessary, national versions of these should be established).

2. Only where no international contributions are found should new national OIO data standards be developed in the manner prescribed by OIO in the OIO-NDR and other relevant OIO guidelines.
- For new and better versions of existing OIO data standards, the principle that international contributions to the new versions should rank higher than national ones is again applicable.

Standards for electronic record management (FESD)

>

The public sector's IT systems at central government, local and regional level should be able to play together in a secure and efficient manner. To meet that need, common standards for electronic file and document handling have been prepared - known as FESD standards.

The aim of this standardisation work is to promote e-government in the public sector, which may be accomplished by ensuring that the various Electronic Record Management Systems (known as ERMS or ERM Systems) get a common core, and also ensuring that further development of this core will proceed a uniform manner. A common core is to ensure:

- that cases can be handled across several organisations,
- that authorities working with open cases can be joined together,
- that tasks can be transferred between different authorities.

Main principle of FESD standards

ERM Systems in the public sector are to be based on a number of standards with the aim of ensuring interoperability to the greatest possible extent between different ERMS and between ERMS and other systems (dedicated systems). So the main objective is for everything to be coordinated in the ERM area in order to ensure higher quality and more efficiency in procedures involving case handling.

Primary scope of FESD standards

The primary scope of mandatory open standards in the ERM area is ERM Systems procured in the public sector.

Mandatory open FESD standards

Mandatory open standards are:

- FESD Cases and Documents
- FESD Address Model
- FESD Exchange Packet
- FESD Scanning Module
- FESD LIS (Management Information)

FESD contains another seven standards, which cannot be made mandatory yet since they have not been finalised. These are:

- FESD Board Handling
- FESD User Administration
- FESD Archive Structure
- FESD Subject Classification
- FESD Secure E-Mail Solution
- FESD Generic Integration Model
- FESD GIS Integration Model

Requirements for use of FESD standards

To use the mandatory open standards for ERMS means:

- that FESD standards are implemented in the manner prescribed in the standards.

>

Maintaining the requirement for use of FESD standards

The OIO catalogue describes, on a current basis, what FESD standards and versions are applicable.

All FESD standards go through a process in which public consultations are a key element. The process of defining specific standards is initiated following a decision by the common public FESD Steering Group. The individual draft standard is then prepared jointly by the so-called FESD suppliers, after which the draft is subjected to public consultation for one month. After adjustment on the basis of the public consultation, the draft standard is submitted for approval.

Standards for electronic procurement in the public sector (OIOUBL)

>

The aim is that trading between the public and private sectors should be fully implemented by using IT and open standards by 2012. To fulfil that aim, the OIOUBL standard has been developed.

It has been developed with the following three business requirements in mind:

- Small and large enterprises and public authorities should be able to handle the basic electronic business documents with a minimum of technological, administrative and economic barriers.
- The business documents should be selected so as to represent the necessary and sufficient set of messages that support the basic procurement process in the public and private sectors.
- The Danish standard should be based on open international standards, so as to enable cross-border trading.

Main principle of electronic procurement

E-business documents in the public sector should be based on a number of standards in order to ensure easy exchange of documents between the public and private sectors. This will enable all suppliers to the public sector to know in advance what format they have to support, and they need only support one rather than several different formats in their IT systems. In return, public authorities get more uniform and structured data, with a potential for further efficiency improvements in work processes and better procurement statistics.

Primary scope of OIOUBL

The primary scope of mandatory open standards for electronic procurement is all public finance and procurement systems acquired by authorities under the agreement on using open standards for software in the public sector.

Mandatory open OIOUBL standards

Mandatory open standards are:

- OIOUBL version 2.01, maintained by the National IT and Telecom Agency.
- UN/SPSC version 7.0401, maintained by GS1.

OIOUBL is a Danish adaptation of the international standard UBL 2.0 from the standardisation body OASIS (Organization for the Advancement of Structured Information Standards) to Danish business requirements. OIOUBL contains standards for all essential business documents to support the procurement process from catalogue to invoice. The documents included in OIOUBL, which form a subset of the UBL 2.0 documents, have been selected in consultation with the Sector Standardisation Committee for e-Business.

UN/SPSC UNSPSC (United Nations Standard Product and Services Code) is an international classification system for products and services. It is used for providing an overview of the resources spent by organisations, and offers systematic search capability in electronic product catalogues. UNDP (United Nations Development Programme) owns the copyright to the UN/SPSC classification system. Day-to-day administration is handled by GS1 US. Jointly with the National IT and Telecom Agency, GS1 Denmark is in charge of the Danish translation of UN/SPSC 7.0401.

>

Requirements for use of OIOUBL

To use the mandatory open standards for electronic ordering means:

- that the OIOUBL specifications are complied with, as described in the National IT and Telecom Agency's guidelines on <http://www.oioubl.info/classes/da/index.html> (Danish version) and <http://www.oioubl.info/classes/en/index.html> (English version),
- that the UN/SPSC classifications are complied with, as described by GS1 on <http://www.ean.dk/unspscdk3/index.htm>.

Standards for digital signatures

>

With digital signatures, the public sector has established a solid infrastructure for secure electronic identification and communication, which is the foundation for e-government and for establishing a new generation of service-oriented public and private Internet services.

By establishing e-services and using digital signatures, the public sector will be able to offer improved services to citizens and businesses, while at the same time increasing the efficiency of the administration.

The OCES standard for digital signatures has been developed in order to break down a number of barriers identified following a previous initiative in 2001 to stimulate the market to use digital signatures to a wider extent based on qualified signatures, cf. EU Directive 1999/93 on a Community framework for electronic signatures.

It appeared in 2001 that the market's business models did not work, notably because citizens were to pay for digital signatures themselves. Other factors were lack of standardisation and poor interoperability across market offerings.

Main principle of OCES digital signatures

As a starting point, public authorities are to base their e-government on the use of OCES digital signatures in connection with the implementation of secure e-mail and self-service solutions that require identification and authenticity. The OCES standard has been defined in OCES certificate policies administered and regulated by the National IT and Telecom Agency. The certificate policies, which have been submitted for public consultation, thus define a standardised and publicly controlled security level for issuing and using OCES digital signatures.

Primary scope of OCES digital signatures

The primary scope of OCES digital signatures is communication between citizens, businesses and the public sector, especially in connection with implementation of secure e-mail and self-service solutions.

Mandatory open OCES standards

Mandatory open standards are:

- OCES personal certificate policy
- OCES employee certificate policy
- OCES company certificate policy
- OCES functional certificate policy

The OCES certificate policies are based on the international standards listed below, but are adjusted in accordance with the legal and administrative requirements of Danish e-government.

CEN Workshop Agreement 14167-2:2002: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

ETSI TS 102 042 v 1.2.1. (2005-05): "Electronic signatures and infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

ETSI SR 002 176 v 1.1.1. (2003-03): "Algorithms and Parameters for Secure Electronic Signatures".

FIPS PUB 140-1: "Security Requirements for Cryptographic Modules".

ISO/IEC 15408 (Parts 1 to 3): "Information technology - Security techniques - Evaluation criteria for IT security".

ISO/IEC 9794-8/ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

Requirements for use of OCES digital signatures

To use the mandatory OCES standard for digital signatures means:

- that secure e-mail solutions using OCES digital signatures are implemented,
- that self-service solutions using OCES digital signatures, where authentication or electronic signatures are needed, are implemented.

Maintaining the requirement for use of OCES digital signatures

The relevant OCES certificate policies are maintained and updated by the National IT and Telecom Agency on a current basis. In case of major revisions, there will be public consultations in connection with the revision.

Current versions of the certificate policies are available on www.signatursekretariatet.dk.

Standards for public websites and accessibility

>

The principles of the public sector's digital communication with citizens and businesses should follow the normal administrative practice, i.e. openness, professionalism and objectivity in the service to citizens.

This means that the public sector's digital communication with citizens and businesses should as far as possible ensure:

- that all parties have equal access to using digital services, and
- that all parties have equal access to communicating with the public sector on a digital basis.

Good administrative practice prescribes that rules and recommendations should as far as possible be written and developed on a neutral basis in terms of technologies and products. Similarly, the public sector should base its e-government offers to citizens and businesses on well-known and available data standards supported by a large number of manufacturers.

In their choice of technology, public authorities should aim at limiting the technical costs and administrative burdens imposed on the citizen or business who wants to communicate digitally with the authorities. Also to be allowed for are the special accessibility needs of citizens and staff with visual, functional or hearing impairments.

As a consequence, all new public websites should be based on internationally recognised open standards.

Main principle of public websites

Public websites should be based on a number of standards in order to ensure accessibility for all citizens and businesses. By using the mandatory standards, it is ensured that the websites are as future-proof as possible and can be used on a broad basis across platforms and tools. And, not least, citizens with permanent or temporary disabilities are ensured digital access to the public sector.

Primary scope of standards for public websites

The primary scope of mandatory open standards for websites is all public websites prepared by authorities under the agreement on using open standards for software in the public sector.

Mandatory open standards for public websites

Mandatory open standards are:

- HTML or XHTML, maintained by W3C (World Wide Web Consortium).
- CSS, maintained by W3C.
- WCAG (Web Content Accessibility Guidelines), latest version, level AA, maintained by WAI (Web Accessibility Initiative) under W3C.

Requirements for use of public websites

To use the mandatory open standards for public websites means:

- that the preferred version of HTML, XHTML and CSS is used in the manner prescribed by W3C,
- that WCAG level AA is complied with.

>

Practical guidelines for compliance can be found on www.itst.dk.

Standards for IT security (DS484)

>

To strengthen the overall IT security in the government sector, all government institutions are to follow a common IT security standard unless special economic or legal conditions indicate otherwise.

Main principle of information security

Government authorities should base the management of their information security on DS484, "Code of practice for information security management".

DS484 is a Danish standard based on the guidelines of the international standard ISO17799:2005 (ISO27002). DS484 contains a number of basic requirements as well as a set of more strict requirements. In order to comply with the standard at least all basic requirements must have been met.

DS484 is a process standard. The choice of specific implementation and solution models in relation to the requirements of the standard is left, to a wide extent, to the individual institution. The starting point for information security is a risk-based approach where risks and solution models are balanced. It is essential for the management to make explicit decisions based on a risk assessment describing what relevance and significance the individual requirements have to the institution and its cooperating partners.

Primary scope of DS484

The primary scope of DS484 is the entire organisation's information processing. Therefore the organisational "footprints" of the standard are not limited to the IT department. In addition, the standard may mean, directly or indirectly, that certain generic requirements have to be met by the organisation's technical installations and physical layout.

Only applicable to the governmental sector

The Government's decision to comply with the standard is mandatory for all institutions that fall within "Executive Order on Public Accounting etc.", referred to as the Accounting Order in the following.

- Under section 2 of the Accounting Order, this comprises all "government institutions, i.e. departments, underlying institutions, special funds etc., and proprietary institutions included in the Appropriation Acts in the same way as regular government institutions". These government institutions are required to follow the common standard for IT security processes.
- Proprietary institutions, associations, funds etc. whose accounts fall within the scope of section 2(2) of the Public Accounts Act are also required to follow the common standard for IT security processes in the government sector where this has been decided by their respective ministries.

Basically, government-owned companies and independent administrative units are not subject to the government system for budgeting and appropriations, and consequently do not fall within the scope of the Government decision.

It should be noted that this requirement applies to more government institutions than those described in the main agreement.

In addition, it should be noted that this requirement does not apply to municipalities and regions.

>

Mandatory open standards for information security

Mandatory open standards are:

- DS484:2005, maintained by Danish Standards

Requirements for use of DS484

To use DS484 means:

- The management of information security has been anchored at chief executive level, partly by establishing a formalised management system - known as Information Security Management System (ISMS), e.g. the system described in ISO 27001.
- A unique responsibility for information security has been placed on the management and, based on a risk assessment, guidelines have been formulated and announced, covering at least the basic requirements of DS484.
- The guidelines have been converted into concrete solutions and/or business procedures which are complied with and being maintained on a regular basis.
- There is regular follow-up on selected indicators of the organisation's security situation, and a suitable level of management information is generated on the basis of this.

Standards for document exchange (ODF/OOXML)

>

Today the exchange of word processing documents between public authorities most frequently employs formats owned by the respective suppliers.

As it is now possible to base the exchange of word processing documents on open formats, the public sector should switch to exchanging word processing documents by using these open formats. This will give wider scope for competition and less dependence on individual suppliers.

Main principle of document standards

Public authorities should be able to receive word processing documents from citizens, businesses and other authorities in the open word processing document formats OOXML and ODF.

IT solutions procured after 1 January 2008 must support at least one of the open word processing document standards ODF and OOXML, and be able to receive word processing documents in both formats, if necessary by using additional programs (converters, plug-ins).

Whether ODF and/or OOXML should be mandatory after 1 July 2009 will be decided following evaluation by an independent third party.

Primary scope of document standards

The primary scope is:

- exchange of editable word processing documents between public authorities, and
- receipt of editable word processing documents from citizens, businesses and authorities.

Mandatory open document standards

The mandatory open standards are:

- ODF (Open Document Format), maintained by the standards organisation OASIS.
- OOXML (Office Open XML), maintained by ECMA.

Requirements for use of document standards

- From 1 January 2008, all authorities must ensure that they can receive documents in these two formats.
- When procuring new systems after 1 January 2008, public authorities must ensure that the systems can support one or both of the formats described.

Maintaining the requirement for use of document standards

Whether ODF and/or OOXML should be mandatory open standards after 1 July 2009 will be decided following evaluation by an independent third party.

This evaluation will include the following:

- The ability of software suppliers to ensure interoperability between the two standards in their products in relation to the exchange requirements of the public sector (functionality ceiling).
- The real possibility of implementing the standards independently of supplier and platform, and the practical experience with this.

>

- A specific evaluation by the Competition Authority on the impact that the use of mandatory open standards for document exchange has on the competitive situation.

The OIO Catalogue is the common public resource to be used for planning and developing public IT projects. The OIO Catalogue contains descriptions and evaluations of selected standards, technologies and protocols desired to be used and supported in connection with the development of e-government in Denmark.

The OIO Catalogue should be known to public authorities developing IT strategies, plans and projects, and to their suppliers and consultants. The intention is to ensure better coherence and technical consistency by using established technologies throughout the Danish public sector.

International anchoring of the OIO Catalogue

Standardisation will often make little sense in a narrow Danish context. One reason is that there is data exchange across borders, and another is that, in practice, standardisation will be carried out by suppliers who address the international market. As a result, standardisation in Denmark must be implemented in continuation of international work in the area.

At EU level, the OIO Catalogue is referred to as a national e-government interoperability framework. A national interoperability framework offers a set of policies, technical standards and guidelines (recommended practice) that outlines the government's policy on how to achieve interoperability. The national interoperability framework addresses all authorities that need to interoperate with other authorities and parties elsewhere, including the EU and other member countries.

Within the European e-government project, a special pan-European interoperability framework has been established (European Interoperability Framework, EIF), which should be seen as a supplement to the national frameworks. The OIO Catalogue has been prepared in line with EIF. There is still a need for continuous adjustment to ensure conformity with EIF.

Adjustments of the OIO Catalogue

The OIO Catalogue has existed under various names since 2003. Developments during the last four years and the requirements in connection with mandatory open standards have made it necessary, naturally enough, to revise the structure and content of the catalogue to reflect the new requirements.

The starting point for introducing mandatory open standards in the public sector is the existing common public standardisation activities. The keyword is continuity, and the introduction of mandatory open standards is basically in line with the standardisation work that has already been going on for several years as a cooperative effort in the public sector, anchored in the National IT and Telecom Agency.

The objective of introducing mandatory open standards is to be achieved through better utilisation and more value being derived from future work with the existing standards. These developments are reflected particularly on three points:

- 1 *Guidance.* So far, the National IT and Telecom Agency has provided guidance on which standards were regarded as the best. Now it will be

mandatory to use certain standards unless significant arguments indicate otherwise. The introduction of the *comply or explain* concept requires public authorities to justify cases in which they do not meet the OIO catalogue's requirements for mandatory standards.

- 2 *Documentation.* There is clearly a need to ensure that decisions on what criteria underlie the approval of standards should be documented to a greater extent.
- 3 *Maintenance.* With a set of mandatory open standards, current focus needs to be placed on developments in the area of standardisation and technical/market-related fields, as well as new business developments.

Structure of the OIO Catalogue

The OIO Catalogue divides standards into three main categories. Technical standards, data standards and process standards.

Characteristics of the three types of standards

Technical standards

It is a characteristic of technical standards that they focus on the *technical* operation of IT systems. The main purpose of establishing technical standards is to ensure technical solutions that support the overall architecture.

Data standards

It is a characteristic of data standards that they focus on the *data* being registered, used and exchanged in various systems and organisations. The purpose of data standards is to provide a basis for more integrated solutions and for reusing data.

Process standards

It is a characteristic of process standards that they focus on the *method* by which work is done in digitalisation projects and in connection with development and operation of IT solutions. It is also a characteristic that there are relatively few process standards. The purpose of process standards is to provide solutions offering quality, coherence, interoperability and confidence.

New mandatory open standards



Mandatory open standards mean selected and named standards found suitable for use in the public sector.

Mandatory open standards are prepared on the recommendation of the Minister for Science, Technology and Innovation and adopted following a decision by the Government and agreement with local and regional authorities.

The decision must be based on a technical and economic assessment of the individual sets of standards.

The technical assessment is intended to clarify if the standard is an open one, what business relevance the standard has to the public sector, and if conditions on the market make the standard ready for use. The technical assessment should be subjected to public consultation.

If the technical assessment shows that the standard is a potential mandatory open standard, a subsequent economic impact assessment must be made in order to clarify if the standard can be adopted as a mandatory, open standard without additional cost to the public sector.

v

Use of Mandatory Open Standards for Software in the Public Sector

From 1 January 2008, it will be mandatory for all public authorities in Denmark to use a number of open standards. This means that all new public IT solutions must be capable of using these mandatory open standards.

As a result, Danish public authorities have to make sure that future IT solutions are based on, or support, these mandatory open standards if the standards are relevant to the IT solution.

All the mandatory open standards are subject to the condition that the individual authority, in case of additional expenses or for reasons of IT security in the authority concerned, may omit to use the mandatory standards
