# Identification of ICT Technical Specifications

## *DomainKeys Identied Mail Signatures (DKIM)*

## Evaluation report

# Management summary

This report contains the evaluation as well as proposed advice of the European Multi-Stakeholder Platform on ICT standardisation ("the Platform") on the submission of the TS DomainKeys Identied Mail Signatures (DKIM) to be identified in accordance with Article 13 and annex II of Regulation (EU) No.1025-/2012. The report assesses compliance against the requirements for the identification of ICT technical specifications, set by Annex II of Regulation (EU) No. 1025/2012. The report should allow the Platform to develop a "positive/negative" advice to the Commission of the submitted technical specification.

Further to the assessments above, it is proposed that the Platform comes to the following conclusion: **a positive advice should be given on the identification of the submitted ICT TS "DKIM".**

# 1. Objective for the report

## 1.1 Background

Economic growth and responsiveness to citizens' expectations in a digital world requires interoperability between services, applications and products. Achieving interoperability requires standards and specifications. Public authorities should make use of the full range of standards and technical specifications when procuring hardware, software and information technology services; this will allow them to efficiently fulfil their tasks. The Pillar II of the Digital Agenda for Europe recognised the need of sound standards and common technical specifications to promote interoperability, and advocates public authorities to make the use of available standards and common technical specifications when commissioning hardware, software and IT services from external suppliers.

To that objective the Regulation 1025/2012 on European standardisation lays down in its Chapter IV a procedure for the identification of ICT technical specifications ICT specifications which are not issued by European, international or national standardisation organisations that could be referenced in public procurement acts, provided that these ICT specifications, proposed by the Commission or by Member States, comply with the requirements set by annex II of the same Regulation.

These requirements cover the coherence of the proposed ICT specification with the formal standardisation environment, the qualities of the standardisation process implemented in the standards setting organisation that issued the proposed ICT specification and some aspects of the proposed specification itself. Compliance with these requirements guarantees the public authorities that the proposed ICT specification are set in accordance with the founding principles recognised by the World Trade organisation (WTO) in the field of standardisation.

The objective for this report is to allow the Platform an evaluation compliance of the proposed ICT specification with the requirements set in annex II of the Regulation. The Platform will subsequently provide its advice to the Commission on the potential identification of the submitted ICT specification.

The Platform is an expert group set up by Commission Decision of 28th November 2011; it is composed of representatives of Member States, industry, societal organisations, formal standards organisation and fora & consortia. Art. 2.f of this Decision states that one of the tasks of the Platform is "*to advise the Commission on the identification of the technical specifications in the field of ICT which are not national, European of international standards*". The Platform agreed on a process for such identification (doc. ICT/MSP (2012) 057), in accordance with art. 13 of the Regulation 1024/2012.

## 1.2 The process

On 22th May 2013 the Dutch Standardisation Forum has submitted the DKIM Signatures as potential ICT specification for identification as ICT specification eligible for referencing in public procurement, in accordance with article 13 of the Regulation. The "identified ICT specification" resulting from the evaluation process, in accordance with art. 14 of the Regulation, shall constitute a "common technical specification" referred to in Directives 2004/17/EC and 2004/18/EC and 2009/81/EC and therefore become eligible for direct referencing in public procurement.

The secretariat of the Platform has the completeness of the information on the evaluation submission form. The submission form has subsequently been forwarded to the members of the Platform for discussion and for the establishment of an evaluation group to assess this information with respect to the requirements set by the Annex II of the Regulation.

The Platform noted the submission of DKIM at its meeting of 13th June 2013 and decided to establish an ad hoc evaluation working group to carefully analyse the data provided by the submission form. If necessary, the evaluation group can seek further information form the submitter and the specification originating organisation to consolidate the information in an evaluation report addressed to the Platform. This report will allow the Platform to prepare its advice on the identification of the proposed ICT specification to the Commission.

The Platform discussed the report and the draft advice at its meeting of 17th October 2013. The Platform secretariat subsequently updated the draft advice in accordance with the outcome of the discussion.

The final draft advice will be submitted for broad consultation to all interested stakeholders via the MSP web site; the consultation will last xxx weeks.

The Platform secretariat will consolidate the comments received during the open consultation and submit to the Platform for further action.

The Platform will, depending on the outcome of the consultation, decide on the finalisation of its draft advice to the Commission or on further discussion within the Platform.

Further to a positive advice of the Platform, the Commission will, in accordance with the internal procedures, prepare the relevant Commission decision on the identification of the ICT specification.

## 1.3 Evaluation group

Following its decision of 13th June 2013, the Platform agreed to establish an evaluation group for DKIM on a voluntary basis. A representative of IETF as specification setting organisation, participated in as advisor; a representative ensured the secretariat of the evaluation group was ensured by a Commission representative.

The evaluation group was composed of the following Platform members:

1. European Commission (secretary)
2. IETF (advisor)
3. DIGITALEUROPE
4. IEEE
5. ECIS
6. Germany
7. Belgium
8. The Netherlands
9. Switzerland

The evaluation group has performed its tasks by electronic means and delivered its preliminary report to the MSP secretariat on 25 October 2013, to be presented to the Platform on its meeting of 17th October 2013.

## 1.4 Subject of the evaluation

This report provides the evaluation of DomainKeys Identified Mail (DKIM) Signatures, RFC 6376 https://tools.ietf.org/html/rfc6376.

DKIM permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. This can be an author's organization, an operational relay, or one of their agents. DKIM separates the question of the identity of the Signer of the message from the purported author of the message. Assertion of responsibility is validated through a cryptographic signature and by querying the Signer's domain directly to retrieve the appropriate public key. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the DKIM signature.

DKIM is developed by IETF (Internet Engineering Taskforce). IETF is the principal body engaged in the developing of the Internet standards. It is a non-profit- organisation without formal membership: members do not pay membership fee and there are no contractual obligations for them. The IETF's standards development work is divided into eight Areas (http://www.ietf.org/iesg/area.html). Each Area has one or more Area Directors (ADs), who together form the Internet Engineering Steering Group (IESG). The IESG is responsible for technical management of IETF activities, the Internet standards process, and for the actions associated with the Internet standards track (Internet standards developing process), including final approval of specifications as Internet Standards and publication as a Request for Comments (RFC). Within each Area there are multiple Working Groups (WG). Each WG has one or more chair who manage the work, and a written charter defining what the work is and when it is due. There are more than 100 WGs. The WGs produce Internet Drafts (I-Ds) which often lead to the publication of an Internet standard as an RFC.

The IETF is a consensus-based group, and authority to act on behalf of the community requires a high degree of consensus and the continued consent of the community. The process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a standard by the appropriate body and is published. In practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality; (2) the need to consider the interests of all of the affected parties; (3) the importance of establishing widespread community consensus; and (4) the difficulty of evaluating the utility of a particular specification for the Internet community. The goals of the Internet Standards Process are:

- technical excellence
- prior implementation and testing
- clear, concise, and easily understood documentation
- openness and fairness
- timeliness.

The goal of technical competence, the requirement for prior implementation and testing, and the need to allow all interested parties to comment all require significant time and effort. The Internet Standards Process is intended to balance these conflicting goals. The process is believed to be as short and simple as possible without sacrificing technical excellence, thorough testing before adoption of a standard, or openness and fairness.

See http://www.ietf.org/about/process-docs.html

## 1.5 Possible links with other ICT technical specifications or standards

While DKIM is a stand-alone ICT technical specification and does not require the implementation of other related standards or specifications to fulfil its purpose, it can be seen as one building block

within an eco-system of technical enablers for secure electronic communications. Accordingly, there are a number of technical specifications that address similar or related applications and that bear touch points with DKIM. The more relevant examples for this are all ICT technical specifications and not all of them dot have formal standards status. However, even these more relevant examples mostly complement or significantly exceed the functionality domain of DKIM, rather than significantly overlapping or even competing with DKIM. Specifically, this includes the following specifications:

- Sender Policy Framework (SPF)[i], IETF RFC 4408: SPF can be seen to be complementary to DKIM in that it enables verification that a message has been sent by a server authorized for this delivery. Whereas DKIM offers authentication of the sending domain on the level of the message itself, SPF offers this authentication at the level of the transmission channel. There are no conflicts between DKIM and SPF and, indeed, the two complementary specifications have been developed and are maintained by the same organization.

- Sender ID, IETF RFC 4406: Sender ID is an authentication protocol with similar functionality to SPF and hence addresses similar applications as DKIM. Sender ID is currently at an experimental stage in IETF as there are some possible incompatibilities with SPF. Implementation of DKIM does not preclude or interfere with implementation of Sender ID

- S/MIME, IETF RFC 5751 and OpenPGP, IETF 3156: S/MIME and OpenPGP enable the encryption and electronic signature of MIME data. This provides for the protection of confidentiality and privacy of electronic communications as well as for the authentication of the sender. They hence go significantly beyond the authentication of the sending domain that is provided by DKIM. Where S/MIME and OpenPGP are applied, application of DKIM is no longer necessary because the functionality is implicitly included in S/MIME and OpenPGP. However, a vast amount of electronic messaging does not require implementation of more involved encryption technologies, but can benefit from the increased confidence in knowing the organizational origin of a message offered by DKIM.

- DKIM Author Domain Signing Practices (ADSP), IETF RFC 5617: ADSP is an informational complement to DKIM.

DNS, DNSSEC: DNS is a hierarchical, distributed infrastructure for networked devices that couples domain names to numerical Internet addresses. DNSSEC is an extension of DNS that provides a security layer for DNS information via a digital signature. DNSSEC can be used to further enhance the security of DKIM applications: DKIM signatures are verified in the public part of the public-private key combination with which this signature is set. That public key is part of the DNS domain of the organization that sets the DKIM signature. Therefore, DNSSEC can provide additional security by offering authenticity and integrity of DKIM public keys. DNSSEC has been proposed for identification at the same time as DKIM and is being evaluated by the MSP in parallel. RFC 4398 "Storing certificates in the Domain Name System (DNS) and the storage of certificates and their usage are however not covered by the DKIM and DNSSEC identification".

# 2 Evaluation of compliance with the general conditions

## 2.1 Market acceptance

DKIM is implemented across several market sectors. DKIM is also being used in the financial and banking sector (BITS, PayPal, Bank of America, ING Bank, Rabobank), by a number of large e-mail providers (such as Yahoo, Gmail, AOL, Hotmail and Fastnet), by a number of social networks (Twitter, FaceBook, LinkedIn, XING, Plaxo, Pinterest) and by a number of Internet commerce providers, such as eBay.

In 2009 the technology policy division (BITS) of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer, adopted a report in which the use of DKIM was recommended to its members (http://www.bits.org/news/pr/BITSSenderAuthenticationPR060909.pdf

A certain market acceptance threshold is also part of the criteria for an IETF specification to reach the status of an Internet standard (see also section 3.2.1.2 below). DKIM holds this status.

Finally, DKIM is a mandatory/required standard for use by public authorities in the Netherlands.

## 2.2 Coherence with the formal European standardisation environment

DKIM is coherent with the formal European standardisation environment as it covers a domain where the adoption of a new European or international standard or standardisation deliverable is not foreseen within a reasonable period. Furthermore, the current scope of the formal European or international standardisation organisations does not cover any similar domain. A transposition of the proposed ICT technical specification into a European or international standard or standardisation is not foreseen within a reasonable period.

# 3 Evaluation of compliance with the attributes

## 3.1 The organisation developing the specification

The specification has been developed and is maintained by the Internet Engineering Task Force (IETF). IETF is a non-profit making organisation. IETF develops standards in the field of ICT, namely Internet related.

What follows is an informal narrative, for a full overview of authoritative documents see http://www.ietf.org/about/process-docs.html

IETF is the leading Internet standards organization. Its aim is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.

IETF is the principal body engaged in the development of new Internet standard specifications. The IETF is unusual in that it exists as a collection of happenings, but is not a corporation and has no board of directors, no members, and no dues; see [BCP95], "A Mission Statement for the IETF", for more detail.

Its mission includes the following:

- Identifying, and proposing solutions to, pressing operational and technical problems in the Internet
- Specifying the development or usage of protocols and the near-term architecture to solve such technical problems for the Internet
- Making recommendations to the Internet Engineering Steering Group (IESG) regarding the standardization of protocols and protocol usage in the Internet
- Facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community
- Providing a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors, and network managers.

IETF is not a traditional standards organization, although many specifications that are produced become standards. IETF is made up of volunteers, many of whom meet three times a year to fulfil the IETF mission. There is no membership in the IETF. Anyone may register for a meeting and then attend. The closest thing there is to being an IETF member is being on the IETF or Working Group mailing lists.

Financial and legal support for the IETF[1] is provided by the Internet Society (ISOC). ISOC maintains the books and is hired the IETF's directly employed administrative staff.

The Internet Society is an international not-for-profit organization concerned with the growth and evolution of the worldwide Internet and with the social, political, and technical issues that arise from its use. The ISOC is an organization with individual and organizational members. The ISOC is managed by a Board of Trustees elected by the worldwide individual membership.

The way in which the members of the ISOC Board of Trustees are selected, and other matters concerning the operation of the Internet Society, are described in the ISOC By Laws [C].

## 3.2 The development process

The Internet Standards Process is documented in RFC2026, as updated by RFC6410.

IETF has no specific membership rules; participation to IETF standardisation activities is open to all on the basis of direct participation. The decision process during specification development is based on what IETF describes as “rough consensus”, which means that the opinion of a technical group, is determined by the chair on the basis of the dominant position in the group. Such determinations can be appealed so that the principle of consensus is indeed safeguarded.

The Internet Standards Process is an **open, transparent, consensus based process**.

### 3.2.1 IETF rules and procedures

1 And the related and/or supporting organisations such as the Internet Architecture Board (IAB), the Internet Research Task Force (IRTF), the IETF Administrative Oversight Committee (IAOC), the Internet Engineering Steering Group (IESG), and the RFC Editor.

#### 3.2.1.1 Standardization process

IETF document BCP 9, found in RFC 2026 and RFC 6410, specifies the process used by the Internet community for the standardization of protocols and procedures. It defines the stages in the standardization process, the requirements for moving a document between stages and the types of documents used during this process. It also addresses the intellectual property rights and copyright issues associated with the standards process.

IETF publishes the RFC series of documents structured as follows:

| Main series | Document status |
|---|---|
| Standards track | |
| | Internet Standard (STD) |
| | Proposed Standard |
| | Best Current Practice |
| Non-standards track | |
| | Informational |
| | Experimental |
| | Historic |

DKIM has already been assigned a standard number: STD 76. DKIM has already been assigned a standard number: STD76. See http://www.rfc-editor.org/rfcxx00.html#STDbySTD

### 3.2.1.2 Standards track maturity levels

DKIM status has meanwhile been elevated from Draft Standard to Internet Standard (STD 76) http://www.ietf.org/mail-archive/web/ietf-announce/current/msg11674.htm . Internet Standards represent the highest maturity level specifications within IETF's standards track.

"Internet Standard" maturity level is attributed to an RFC after confirmation of the following criteria:

a) There are at least two independent interoperating implementations with widespread deployment and successful operational experience.
b) There are no errata against the specification that would cause an implementation to fail to interoperate with deployed ones.
c) There are no unused features in the specification that greatly increase implementation complexity.
d) If the technology required to implement the specification requires patented or otherwise controlled technology, then the set of implementations must demonstrate at least two independent, separate and successful uses of the licensing process.

The IETF Standards Process no longer requires a formal interoperability report, recognizing that deployment and use is sufficient to show interoperability.

"Proposed Standard" is the entry-level maturity for the standards track. A specific action by the IESG is required to move a specification onto the standards track at the "Proposed Standard" level.

### 3.2.1. Openness

Any interested party can join mailing lists (with public archives) without charge and participate in the development of the specification and the development of the consensus. Face to face meetings are organized 3 times per year[2] and allow for remote participation.

### 3.2.2. Consensus

IETF Standards are subject to IETF consensus as judged by the Internet Engineering Steering Group (IESG), a management body consisting of 12 members. The consensus determination includes a 2 or 4 week '*last call*' on the public IETF mailing list. Determination of consensus can be appealed through a well-defined 3 step appeal process (involving the IESG, the Internet Architecture Board –IAB-, and ISOC).

### 3.2.3. Transparency

Public archives of the mailing lists are maintained, records of meetings are published in proceedings, and decisions by the IESG are made available publicly.

## 3.3 The specification

### 3.3.1. Maintenance

Updating of a specification is done through the publication of a new set of RFCs.

IETF exists since 1986 and has proven to be a stable organisation, which has been developing and maintaining standards over a long period. The various specifications are maintained in the different relevant working groups part of the IETF structure.

It should be pointed out that no review cycle is imposed on Standards Track documents at any maturity level. Updating of specifications is undertaken upon request from IETF members.

In the case of DKIM, the working group is closed. However, there is still a mailing list active for discussion about DKIM within IETF.

### 3.3.2. Availability

All IETF specifications are available for free download from http://www.rfc-editor.org/

The ones related to DKIM can be found in:

2 Sometimes working groups organize interim-meetings.

http://datatracker.ietf.org/doc/status-change-dkim-to-internetstandard/

### 3.3.3. Intellectual Property rules

The IETF intellectual property rights rules are defined in RFC 3979 (http://www.rfc-editor.org/in-notes/rfc3979.txt), "Intellectual Property Rights in IETF Technology" (updated by RFC 4879 (http://www.rfc-editor.org/in-notes/rfc4879.txt), "Clarification of the Third Party Disclosure Procedure in RFC 3979").

The policy with respect to IPR (patents) can be summarized as followed:

The IETF takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology described in any IETF documents or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Contributors to the IETF process are expected to disclose the existence of IPR in technology.

The IETF Executive Director is expected to receive written assurance that a FRAND license (possibly royalty free) will be made available, or that no license will be required. In fact, while there is a preference for royalty-free licensing, the IETF working groups may opt to prefer technology that is known to have FRAND or even no known licensing terms.

The absence of IPR disclosures is not the same thing as the knowledge that there will be no IPR claims in the future. The validity and enforceability of any IPR may be challenged for legitimate reasons, and the mere existence of an IPR disclosure should not automatically be taken to mean that the disclosed IPR is valid or enforceable. In fact IETF Working Groups will take into account on their own opinions of the validity, enforceability or applicability of IPR in their evaluation of alternative technologies.

The IETF's licensing policy is nuanced and in a summary it is not possible to describe in detail those nuances; the reader is advised to carefully read 3979 if there are any concerns.

Participants to the IETF process are being made aware of the IPR policies by means of the so called "NOTE WELL" that is shown at working group meetings, during registration, when subscribing to a mailing list, etc.

More specifically for DKIM see: http://datatracker.ietf.org/ipr/1615/ which describes Yahoo's commitment to license its essential patent(s) in DKIM under the (royalty-free) Gnu General Public License V2.0.

### 3.3.4. Relevance

As attested by its broad market acceptance, DKIM effectively caters for a relevant market need.

DKIM is listed as open standard for referencing in public procurement by The Netherlands (https://lijsten.forumstandaardisatie.nl/).

This listing is based on a thorough assessment of the specification and its relevance to public authorities. As explained in the report by the expert group, DKIM's use by public authorities can significantly contribute to improving interoperability – when public authorities e.g. government agencies use DKIM, the receiver of these messages can be sure that the communication is from a

trusted party. As the report also explains, a great number of communications from public authorities to citizens are not using and do not warrant the use of advanced encryption-based security protection. DKIM offers a light-weight and inexpensive method to nevertheless establish a basic level of trust in the origin of such communications. That way, interoperability between sending- and receiving organizations improves, to get the mail in the inbox of the receiver.

### 3.3.5. Neutrality and stability

DKIM is a performance oriented specification that does not prescribe design or other descriptive characteristics of implementations. The specification is based on state-of-the-art scientific and technological developments. DKIM does not limit the possibilities for implementers to develop competition and innovation based upon it; it rather represents one building block for electronic communication security that can be complemented and enhanced with other technologies. There are no indications for any market-distorting potential arising from the use of DKIM.

### 3.3.6. Quality

As the adoption by various different players in the market demonstrated, the quality and level of detail of the DKIM specification are sufficient to permit the development of a variety of competing implementations of interoperable products and services. Standardized interfaces are not hidden or controlled by anyone other than the organization that adopted the technical specification.

# 4 Summary and conclusion

The evaluation working Group has evaluated the "DKIM specification".

The group is of the opinion that DKIM complies with the requirements for the identification of ICT technical specifications set by Annex II of Regulation (EU) No. 1025/2012.

In particular, DKIM fulfils the general conditions indicated in the Annex II, i.e., has market acceptance and is coherent with the standards published by the formal European standardisation organisations, i.e., there is no duplication with existing standards or on-going standardisation activities. The proposed ICT specification is coherent with the European standards established by CEN, CENELEC and ETSI. The organisation that develops the DKIM, IETF, complies with the attributes referred in the Annex II, i.e., is an open, transparent, non-profit organisation with expertise in developing standards in the field of ICT. Participation to IETF standardisation activities is open to all interested parties. Decisions are based on consensus building within the technical committees; IETF is taking care of maintenance. The IETF specifications are freely available for download. IETF does not impose IPR on its specifications. IETF favours that IPR are provided licence-free of licensed in a FRAND basis. All of these principles were in particular applied to the development of DKIM.

DKIM is a stable technology, there is ample expertise available with respect to the use.

DKIM has the potential to increase interoperability; implementing DKIM may contribute to avoidance of vendor lock in because it provides a specified way of adding domain authenticity to e-mail communications that is open to use by any party.

The implementation of DKIM will improve the better accessibility and continuity especially for public services to be delivered by the public administrations because it can enhance trust in the authenticity of communications from public authorities. Continuity with future development is guaranteed.

**Therefore the Platform issued a positive advice on the identification on DKIM as common technical specifications in the sense of art. 14 of the Regulation 1025/2012.**

[i] SPF in RFC4408 got the status "experimental" as there was a conflict in the use of the DND record. At this very moment the spfbis working group within the IETF has produced a new version, which is now in the "last call". It will be published as "Standards Track" (i.e. Proposed Standard).