



FORUM STANDAARDISATIE

Expert Recommendation

SAML v 2.0

Author(s)

A.C.M. Smulders, D. Krukkert

Date

19 February, 2009

Version

1.2

Status

Final

Contents

Management summary	3
1. Expert recommendation objective	4
1.1 Background	4
1.2 Process	4
1.3 Composition of the expert group	5
1.4 About SAML	6
2. Area of application and organisational scope	7
2.1 Area of application	7
2.2 Organisational scope	Fout! Bladwijzer niet gedefinieerd.
3. Evaluation of the standard based on the criteria	9
3.1 Openness	9
3.2 Usability	Fout! Bladwijzer niet gedefinieerd.
3.3 Potential	13
3.4 Impact	13
4. Recommendation to Forum and Board	15
4.1 Summary of evaluation criteria	15
4.2 Recommendation	15

Management summary

This report contains the recommendation of the SAML expert group to the Standardisation Forum and the Standardisation Board on including the SAML v2.0 standard in the list of open standards.

The expert group has come to the conclusion that SAML v2.0 can be included in the list of open standards.

The most important aspects of this recommendation are as follows:

- Using SAML v2.0 will make the standard exchange of information between parties easier and more univocal. This will enhance interoperability and reduce the risk of errors in the information supply.
- The expert group recommends not including any restrictions with regard to the organisational scope of the SAML v2.0 standard. The organisational scope would then cover all organisations to which the 'Comply or Explain' principle applies: government organisations and all other (semi-)public institutions.
- The area of application of the standard includes federative browser-based single sign-on and single sign-off. In practice, this will be the main focus of the standard's application. Other areas of application, such as enterprise single sign-on, are not the standard's primary focus.
- The SAML v2.0 standard meets the proposed criteria with respect to openness, usability, and potential.
- The area of application affects the business operations, as the interdependence increases due to a new collaboration method within the government.
- Implementation of the standard impacts the organisational setup, which therefore must be reassessed. Topics to be covered in this context include which organisations can make which claims regarding a person, what these claims mean, and how they are verified.
- SAML v2.0 provides security functionality and will therefore be applied in areas where security and privacy play a role. This means that within the area of application, the considerations on which implementation decisions are based must undergo a critical assessment, as these can have a significant impact on security and privacy.



1. Expert recommendation objective

1.1 Background

On Monday, 17 September 2007, the Dutch State Secretary of Economic Affairs sent the action plan for open standards and open-source software to the Lower House. The purpose of the action plan is to make the information supply more accessible to achieve independence from IT suppliers and facilitate innovation.

One aspect of the action plan is compiling a list of standards governed by the 'Comply or Explain' principle. The Standardisation Board decides which standards will be included in the list, based in part on an expert evaluation of the standard.

The experts are part of a balanced expert group that evaluates the standard based on a number of criteria. These criteria, as well their specification in the form of concrete questions, are included in this expert recommendation and have been taken over from the VKA report *Open standaarden: het proces om te komen tot een lijst met open standaarden* (Open standards – the process for creating a list of open standards). This report was approved by the Standardisation Board on 14 May 2008 and can be found on the website of the Standardisation Forum.

The expert group's task was to provide a recommendation on whether SAML version 2.0 (hereinafter referred to as SAML v2.0) should be included in the list of open standards, with or without specific conditions.

1.2 Process

The following procedure was used to define this recommendation.

The expert group started by individually scoring SAML v2.0 based on a questionnaire. This questionnaire contains the criteria outlined in the above-mentioned report. Based on the answers given, the chairman of the expert group identified the bottlenecks.

Next, the expert group held a meeting on 19 January 2009 for a general discussion of the outcome and, in particular, the bottlenecks identified. During this meeting, the area of application and the organisational scope were defined.

The findings of the expert group were included in this recommendation report by the chairman and monitor member. A first draft version was sent to the members of the expert group with a request for response. The feedback received was incorporated in the report and the finalised version was submitted for the public consultation phase.



1.3 Composition of the expert group

Experts and other persons who are directly or indirectly involved with the standard due to their personal expertise or work at a particular organisation were invited to join the expert group. In addition, an independent chairman was appointed to lead the expert group and act as the responsible party for the final expert recommendation.

Andre Smulders was appointed chairman. He is a senior consultant at TNO Information and Communication Technology. In his present role, he works on information security projects, varying from a technological to a strategic level. He is also the co-writer of a basic book on information security, which was published under a 'Creative Commons' licence. Michael van Bekkum, consultant at TNO Information and Communication technology, acts as counsellor to the expert group. Dennis Krukkert is a consultant at TNO Information and Communication Technology.

The members of the expert group were:

- Jeroen de Beer (Anoigo)
- Lex Borger (Logica)
- Hans Bos (Microsoft)
- Marnix Dekker (GBO, DigiD programme)
- Barry Dukker (IVENT)
- Henk Geurtsen (UWV WERKbedrijf)
- Bart Kerver (ICTU, PIP programme)
- Rene Klomp (SUN Microsystems)
- Bart Knubben (VKA)
- Jacqueline Kok (Atos Origin)
- Jaap Kuipers (Surf)
- Jeroen de Miranda (Siemens)
- Rob van der Staaij (Atos Origin)
- Peter Valkenburg (Everett)
- Ton Verschuren (Innofusie)
- Erik Vullings (TNO)



- Maarten Wegdam (Telematica Institute)
- Hans Zandbelt (Surf)
- Frank Zwart (ICTU, PIP programme)

1.4 About SAML¹

The assessed standard was developed by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS). The Security Assertion Markup Language (SAML) is an XML-based framework for communicating user authentication, rights, and attribute information. SAML provides organisational entities with the possibility to make claims regarding the identity, attributes, and rights of a subject (an entity that is often a human user) to other entities such as internet applications or services. An example of an authentication claim is:

“Subject Bob was authenticated at 9.03 a.m. based on an X.509 certificate.”

SAML defines the syntax and processing semantics of claims made by a system entity regarding a subject. When assessing the dependence of these claims, SAML system entities can use other protocols (including SOAP) to communicate regarding a claim or the subject of a claim.

The expert group assessed version 2.0 of the SAML standard.

¹ Text is based on: S. Cantor et al. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS SSTC, March 2005. Document ID samlcore-2.0-os. See <http://www.oasis-open.org/committees/security/>. And: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security



2. Area of application and organisational scope

Government organisations are expected to use the list of open standards during tendering procedures, according to the 'Comply or Explain' principle. Depending on the functionality to be acquired, a decision will be made as to which interfaces must be implemented, and which standards from the list should be applied to this end. For this purpose, the expert group evaluated in which cases the functionality of SAML v2.0 should be used (area of application), and which organisations should use SAML v2.0 (organisational scope).

2.1 Area of application

The expert group has decided to keep the functional organisational scope of SAML intact. This means that SAML v2.0 can be deployed for the exchange of authorisation and authentication data between security domains.

As the area of application, the expert group has chosen 'federative (web) browser-based single sign-on (SSO) and single sign-off'. This means that after a user signs in via the browser, they have access to multiple services from different parties.

When establishing the area of application, the expert group took the following aspects into consideration:

- SAML standard has a broad potential area of application. SAML v2.0 provides more functionality than SSO alone. It also provides the possibility to share attributes, and can be used for access control and authorisation purposes (possibly in combination with eXtended Access Control Markup Language (XACML), which provides more detailed possibilities).
- In practice, the main area of application of this standard turns out to be the application of SAML in federative browser-based single sign-on. SAML also provides the basis for single sign-off (the user signs off from all applications with one action), within the framework of federative browser-based information systems.
- For other functional areas of application, including enterprise single sign-on and web service security, other standards are available or under development. The expert group is of the opinion that the 'Comply or Explain' principle for SAML v2.0 is too heavy for these other areas of application, and does not do justice to the other standards such as Kerberos and WS-Federation. A process is currently being carried out to realise compatibility between SAML v2.0 and WS-Federation. It is therefore not possible at this point to make any assessment regarding which standard is most suitable within that area of application.



2.2 Organisational scope

With respect to the selected area of application, the expert group does not deem further demarcation of the organisational scope necessary. This means that the organisational scope covers all organisations to which the 'Comply or Explain' principle applies, i.e. government organisations and institutions in the (semi-)public sector².

² As defined in the action plan *Nederland Open in Verbinding* (The Netherlands Open in Connection)



3. Evaluation of the standard based on the criteria

A number of criteria were used to decide whether SAML v2.0 should be included in the list of open standards. These criteria are described in the report *Open standaarden, het proces om te komen tot een lijst met open standaarden* (Open standards – the process for creating a list of open standards). This report was created by Verdonck, Klooster & Associates and was published on 23 April 2008. The result of the assessment is outlined per criterion in this chapter. For the sake of completeness, the definition of each criterion has been included in *italics*.

3.1 Openness

Approval and enforcement

The standard has been approved and will be enforced by a non-profit organisation. Ongoing development is based on a decision-making procedure which is open to all stakeholders (consensus or decision by majority, etc.).

The SAML 2.0 standard is approved and maintained by the non-profit consortium OASIS (Organization for the Advancement of Structured Information Standards). OASIS strives for convergence and adaptation of open standards in the area of web services. OASIS was established in 1993 and has over 5,000 participants from more than 600 organisations and individual members in 100 countries.

OASIS has transparent governance and operational procedures. The technical agenda is established by the members within a process that aims to establish industry consensus and focused efforts. Finished work is ratified by an open round of approval. Governance is accountable and is not subject to any restrictions. The OASIS board and the Director and technical advisory board are elected for a period of two years via a democratic process. Consortium leadership is based on individual contributions and is not restricted by financial contribution, business role or special appointment.

Availability

The standard has been published and its specifications document is freely available or can be acquired at a nominal fee. Anyone must be able to copy and use the document and make it available for free, or at a nominal fee.

Anyone can access the standard for free via the OASIS website.



Intellectual property

The intellectual property – with respect to any patents that may exist – of (parts of) the standard is irrevocably made available on a royalty-free basis.

The expert group believes this criterion is complied with sufficiently, although, strictly speaking, patents are not made available irrevocably.

Aspects taken into account by the expert group include the following:

- From enquiries made to OASIS, it transpired that full compliance with this criterion is not possible, if only due to the fact that any patents of organisations outside OASIS lie outside the organisational scope of OASIS. Making patents available royalty-free is only possible for organisations that are directly involved in the development of the standard, and members of OASIS (who have signed a statement to this end). However, the expert group is of the opinion that this is not an objection for inclusion on the list, partly because this applies to almost all standards.
- In order to ensure (legal) certainty, a lawyer will need to be consulted. It is, however, highly likely that full compliance will be possible (as is the case for many standards). It is not possible to provide 100% certainty that no other organisation in the world will ever make a claim regarding any patent violation. Denmark uses similar criteria for openness and has also adopted SAML.

Reuse

There are no restrictions with respect to reuse of the standard.

There are no additional requirements with respect to use of the standard. Although, in theory, no guarantee can be provided with respect to possible patent claims (as mentioned above), since the introduction of the standard there have been no known cases where restrictions have caused conflicts with respect to use of the standard.

3.2 Usability

Maturity

Is the standard sufficiently mature?

Yes, the standard has evolved into version 2.0. The expert group indicates that this makes the standard sufficiently mature.

Are further development and maintenance of the standard guaranteed?

Yes, the organisation maintaining the standard (OASIS) has proved to be a stable organisation able to develop and maintain standards over a long period.



Is there a method for assessing conformity with the standard?

Yes, several methods are available for assessing conformity with the standard. Compared to other standards, this indicates that the maturity of SAML v2.0 is more than sufficient.

Within the expert group, the following methods are mentioned for assessing conformity:

- Based on the conformity document made available by OASIS (<http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>). Although assessment based on the conformity document does not completely fit in the area of application (the entire standard is assumed to be implemented), it does provide a sufficiently wide range of possibilities. Within OASIS, a conformance assessment is being developed that will correspond more closely with the practical use of SAML v2.0. In the long term, more specific tests are expected to emerge for the area of application.
- XML messages can be checked based on the SAML XSD.
- Implementations can be easily checked via the Liberty Interoperable programme: http://projectliberty.org/index.php/liberty/liberty_interoperable.
- Via tests.

Is there sufficient practical experience with use of the standard?

Yes, the standard is included in many standard products, and most suppliers that operate in the relevant field of activity provide support.

In addition to its own knowledge and experience, the expert group names a few initiatives that support this:

- In its *Liberty alliance global adoption newsletter*, volume VI, autumn 2007, the Liberty Alliance organisation concludes that an increasing number of governments (the United States, Denmark, Australia, and New Zealand) are adopting the SAML 2.0 standard. As a result, specific government profiles become available. The Liberty Alliance indicates that the development of a government-approved 'government profile' is challenging, but also offers great opportunities.
- In New Zealand, the development of a deployment profile of the SAML v2.0 specification has been in progress for some time now. The result includes user-controlled, privacy-based policy and design decisions.
- SAML v2.0 has also received attention at a European level. ENISA has published a report on the suitability of SAML v2.0 for expressing Authentication Assurance Levels (AALs). The



report is a response to an appeal made by the Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens (IDABC). The IDABC is a programme that is managed by the Directorate-General for Informatics of the European Commission. The IDABC has published a proposal for a set of four Authentication Assurance Levels (AALs), each of which represents a certain strength for an authentication process. The objective of the ENISA report is to obtain more knowledge on the options available to express AAL in terms of SAML v2.0.

- The applicability of SAML v2.0 is also investigated within the eID/STORK project, which is managed by IDABC. The goal is to examine the possibilities of an implementation of an EU-wide interoperable system for recognition of eID and authentication. This is seen as an enabler for companies, citizens, and government officials to use their national electronic identities in each member state.
- The fact that some suppliers deliver products that (partly outside the chosen area of application) support several standards does not change the practical experience with the SAML standard.

Does the standard have sufficient support from (multiple) market parties now, and will it also receive this support in the future?

Yes, an increasing number of market parties are implementing this standard, mainly because user organisations are also adopting it. See above for additional information.

Are expectations for future use of the standard favourable?

Yes, see above for additional information.

Functionality

Does the standard meet the functional requirements for use of the standard within the proposed area of application?

The area of application is defined in such a manner that the selected functionality of the standard is the part that is currently most widely used. The general consensus is that based on this demarcation, there are no competing standards. Outside the applied demarcation, there are competing standards (see below).

Competing standards



Are there any competing standards? If so, what are they and who uses them? What are the advantages and disadvantages of this standard compared to competing standards?

No, the selected functional demarcation does not comprise any extensive alternatives. WS-Federation is an alternative for a part of the area of application, but is almost exclusively used in Microsoft environments and has not reached the same level of maturity as the SAML v2.0 standard.

3.3 Potential

Does inclusion of the standard in the list contribute to increased supplier independence?

Yes, inclusion of the standard in the list makes products of multiple suppliers increasingly interchangeable.

Does inclusion of the standard in the list contribute to increased interoperability?

Yes, inclusion of the standard in the list contributes to increased interoperability.

In addition to inclusion of SAML in the list of standards, the expert group recommends the following:

- If additional agreements are made regarding certain implementation options offered by SAML, the interoperability can be further increased.

3.4 Impact

The questions on impact can be summarised as follows:

How does the standard impact the business operation, information supply, IT, and the security and privacy of the users of the standard? How difficult is it to migrate to the standard?

The main risk of federative browser-based SSO is the increased dependence on others. For instance, if the central Identity Provider (IdP) does not work, signing in is not possible with any Service Provider. This will require attention in the business operations. The increased dependence is not primarily caused by the SAML v2.0 standard; it is more a result of the new way of collaborating within the government. Furthermore, the expert group concludes that the risks of the standard are primarily the result of the complexity of the SAML v2.0 standard. Like with any other (complex) standard, this poses risks to the (technical) implementation.

Implementation of the standard requires that the organisational setup be reassessed. Topics to be covered in this context include which organisations can make which claims regarding a person, what these claims mean, and how they are verified.



SAML v2.0 provides security functionality and will therefore be applied in areas where security and privacy play a role. This means that for each implementation within the area of application, the considerations on which implementation decisions are based must undergo a critical assessment. Furthermore, SAML v2.0-specific risks (and measures) can be identified in the field of security and privacy. Within the standard, this is discussed in the following document: <http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf>.

Many of the risks outlined above apply to all applications in which identity(-related) data is processed. In general, the expert group believes these risks to be much lower than the risks of not using the SAML v2.0 standard.

Using the SAML v2.0 standard will make the exchange of information between parties easier and more univocal, reducing the risk of errors in the information supply.

The standard offers the option of anonymous authentication³. This is an implementation decision that must be based primarily on the requirements of the government and the applicable frameworks, such as the Personal Data Protection Act. In addition, the SAML v2.0 standard offers room to implement the standard in different ways, for instance anonymity and pseudonymity. It is not always clear to users which data is sent. Although SAML v2.0 does provide the possibility to make this visible, this must be taken into account in implementation of the standard (this problem is generic for this type of systems). The expert group expects the main privacy risks to occur in relation to the central IdP role.

With regard to the migration of existing services to this standard, legacy applications may not need to be adjusted, depending on the setup. It is also possible to wrap existing applications to enable SAML v2.0 to be 'communicated' outwards. In some cases, backwards compatibility of facilities such as DigiD may need to be taken into account. This will require attention in the event of a migration to SAML v2.0.

³ The identity is known to the Identity Provider.



4. Recommendation to Forum and Board

4.1 Summary of evaluation criteria

In summary, the outcome of the evaluation of the criteria is as follows:

– *Openness*

The standard meets the criteria for openness. Strictly speaking, the condition of royalty-free availability of all patents that may be involved is not met, because this is partly outside the control of the managing organisation, as no guarantee can be given that there will never be an organisation putting forward a patent claim. This does, however, not hinder inclusion in the list, partly because the expert group is not aware of any instances in which restrictions have caused conflicts.

– *Usability*

SAML is a mature standard that is widely supported and used. SAML complies with the requirements that apply within the chosen area of application. Within this area of application, no alternative standard is available that realises the same functionality and level of maturity.

– *Potential*

SAML offers sufficient potential with respect to improving interoperability. It also enhances supplier independence.

– *Impact*

SAML is deployed in environments for federative browser-based SSO, which results in a certain dependence on other parties. In these environments, aspects such as security and privacy play an important role as well. This is not an immediate consequence of the implementation of SAML, but it does require a critical eye in the event of implementation decisions.

Depending on the implementation of SAML, it may not always be clear to the end-user which data is sent. SAML does offer solutions for this issue, but users are not forced to use them.

The expert group believes the risks of the above-mentioned aspects to be lower than the risks posed by the alternative – not choosing SAML.

4.2 Recommendation

The expert group advises the Board to include SAML v2.0 in the list of open standards. A few minor issues have been identified, but these do not hinder inclusion.