ISO/IEC JTC 1/SC 27/WG 5 N1320

REPLACES:N1284

ISO/IEC JTC 1/SC 27/WG 5

Information technology - Security techniques - Identity management and privacy technologies

Convenorship/Secretariat: DIN, Germany

Document type:	**Standing Document**
Title:	**Text for WG 5 Standing Document 4 (SD4) -- Standards Privacy Assessment (SPA)**
Status:	**Updated document based on draft disposition of comments received from WG 5 N1189 Att1 and N1189 Att2. It is being circulated for consideration at the 26th SC 27/WG 5 meeting in Gjøvik, Norway, 2018-09-30/10-04.**
Date of document:	2018-09-26
Source:	**SD4 Editors (Frank Dawson, Rajeev Thykatt)**
Expected action:	**ACT**
Action due date:	
No. of pages:	1 + 8
Email of secretary:	**krystyna.passia@din.de**
Committee URL:	http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg5

ISO/IEC JTC1/SC27/WG5 N1284

Standing Document 4
Standard Privacy Assessment (SPA)

Contents

Introduction

This document is a Standing Document (SD) that defines a Standards Privacy Assessment (SPA) process. The SPA process provides guidelines for creating a Privacy Considerations section within WG5 standards. This SD may be modified from time to time, based on comments from national body and liaison contributions.

1 Scope

ISO/IEC JTC1/SC27 is chartered with the development of standards for the protection of information in Information and Communication Technology (ICT) systems. These standards may have privacy impact, in which case they will need to be developed to protect the Personally Identifiable Information (PII) of the consumers who trust in this technology. The Standards Privacy Assessment (SPA) Standing Document provides standard and specification Editors with guidance on:

- Why a Privacy Considerations section is needed in standards and specifications,
- When a SPA process should be used for a standard and specification,
- How to conduct a SPA analysis on a standard and specification, and
- What findings should be included in the Privacy Considerations section of a standard and specification.

The privacy impact of a standard or specification is directly related to either PII or technical mechanisms for identifying information that can be linked to the data principal associated with that information.

The SPA is a methodology assessing the possible privacy impact(s) of a standard or specification. It considers applicable privacy principles and associated privacy safeguarding requirements in order to assess the potential threats arising from the standard or specification that require mitigation by introducing privacy safeguards or controls. In addition, the SPA process is intended to help create information that will be used in analyzing the potential harm towards an individual that could be caused by the technology defined by the standard or specification.

2 Terminology

personally identifiable information
PII

any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

[Source: ISO/IEC 29100:2011]

PII principal

natural person to whom the personally identifiable information (PII) relates

[Source: ISO/IEC 29100:2011]

threat

potential cause of an unwanted incident, which may result in harm to a system, individual or organization

[Adapted from ISO/IEC 27000:2009]

threat agents

an individual or group of individuals who have any role in the execution of a threat

[Adapted from ISO/IEC 27032:2012]

vulnerability

weakness of an asset or control that can be exploited by a threat

[SOURCE: ISO/IEC 27000:2009]

3 Guidance to Editors on when to apply SPA

The work of SC 27/WG 5, as taken from [1], covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and privacy, as well as the identification of requirements for and development of future standards and guidelines in these areas.

In meeting the mandate of SC27/WG5, Editors of SC27/WG5 standards and specifications will need to consider the privacy impact of their work.

In addition, when SC27/WG5 participants liaise and collaborate with other organizations and committees dealing with work similar to that of SC27/WG5, the participants need to be mindful when their collaboration topics have a privacy impact.

The following logic diagram may be useful to an Editor or SC27/WG5 participant to determine the privacy impact of the work they are involved in.

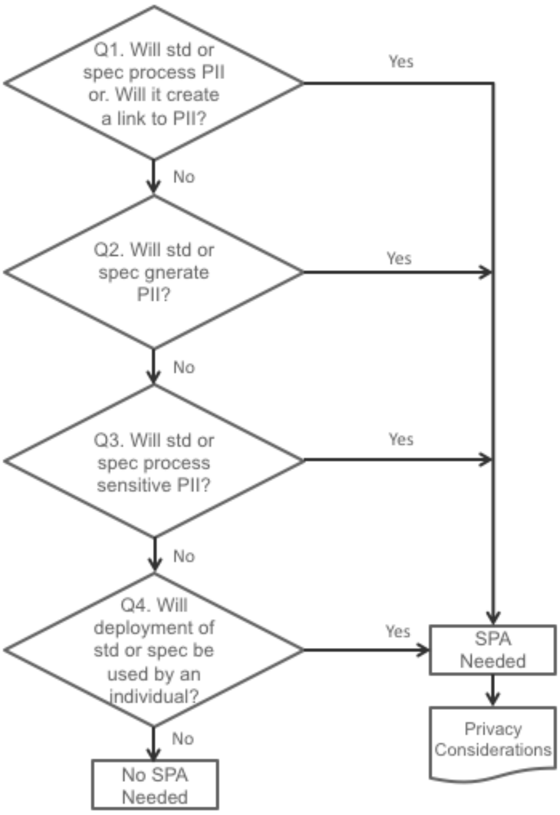
Q1. Will std or spec process PII or. Will it create a link to PII?
Yes
No
Q2. Will std or spec gnerate PII?
Yes
No
Q3. Will std or spec process sensitive PII?
Yes
No
Q4. Will deployment of std or spec be used by an individual?
Yes
No
SPA Needed
Privacy Considerations
No SPA Needed

Figure 1: Determining when to apply SPA

In order to determine whether to apply the SPA process, three questions need to be answered concerning the Standard or Specification Under Review (SUR). First, will the SUR involve technology that will process PII, or will it involve technology that could link information to an identifiable individual? Second, if the SUR will not process PII or involve technology that could link information to an identifiable individual, will it generate PII? Third, if the SUR will not generate PII, will it involve technology that will be used in a network device by an individual? If the answer to any of these questions is affirmative, then the SPA process should be applied to the SUR.

In the event that a SPA process is not considered warranted, then the Privacy Considerations section should clearly articulate this using text such as the following:

> "This standard [or specification] does not define technology that will process Personally Identifiable Information (PII), nor will it create any link to PII. Furthermore, the standard [or specification] does not define technology that will be deployed in a network device and used by an individual."

4 Application of SPA at SC27 standards development milestones

Figure 2 illustrates the ISO standards development process used in ISO/IEC JTC1/SC27 [1].

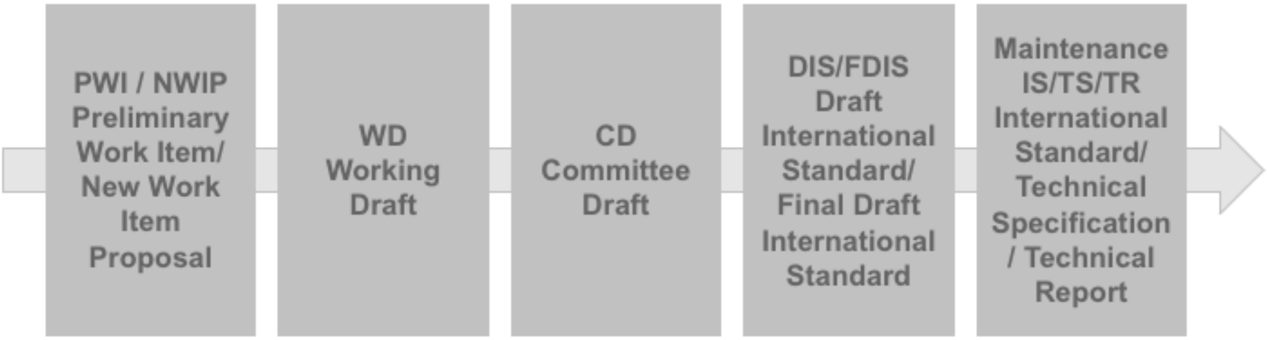
PWI / NWIP Preliminary Work Item/ New Work Item Proposal
WD Working Draft
CD Committee Draft
DIS/FDIS Draft International Standard/ Final Draft International Standard
Maintenance IS/TS/TR International Standard/ Technical Specification / Technical Report

Figure 2: SC27 standards development milestones

The application of the SPA process should not wait until the final milestones but instead should be applied from the first milestone, when a Study Period or New Work Item Proposal is being developed. The various activities that apply to each milestone include:

Study Period/ Preliminary Work Item and New Work Item Proposal

- The best time to start the SPA is when the new work item is being created,
- The new work item should include an explanation of relevant privacy fundamentals, privacy goals and the SPA process, and
- A Privacy Champion for the standard or specification should be identified.

The Privacy Champion is a member of the project team who is responsible for ensuring that the privacy considerations section for the standard is properly developed and documented.

Working Draft

- The International Standard, Technical Specification or Technical Report takes shape through contributions, and
- As the project team creates functionality for the standard or specification, data flows are analyzed and categorized, areas for Privacy Engineering are identified, privacy requirements are identified, threats are identified, safeguards are defined, and findings documented in SPA report.

Committee Draft or Proposed Draft Technical Report

- The International Standard, Technical Specification or Technical Report Editor and project team ensures that the Privacy Considerations text addresses all of the issues and mitigation steps identified during the SPA process, and where appropriate/necessary, make changes to the text.

Draft International Standard/ Final Draft International Standard

- The ISO publication staff and International Standard, Technical Specification or Technical Report Editor verify Privacy Considerations is consistent with ISO/IEC Directives, Part 2 -- Rules for the structure and drafting of International Standards and where appropriate/necessary makes changes to the text accordingly.

Maintenance of International Standards/Technical Specifications/Technical Reports

- Deployment of the standard or specification may lead to the reporting of privacy issues that need to be addressed in a timely manner through requests for changes to the standard or specification.

5 SPA process

The SPA process involves the following analytical steps:

1. Create a clear understanding of the description of the technical functioning of the SUR,

2. Identify the data flow(s) between internal components (interactors) of the SUR and external components (interactors),

3. Classify the data identified in Step 2 to understand the data processed (i.e., the Privacy Data Lifecycle defined by ISO 29100 – Privacy Framework) and whether the SUR features can identify, link to, or through observation otherwise determine the person associated with the PII,

4. Identify applicable privacy principles and associated privacy safeguarding requirements from [2] that apply to the primary use cases for the SUR,

5. Identify the threats created by analyzing the data flows from Step 2, along with the data classification from Step 3 and the applicable privacy requirements from Step 4,

6. Identify appropriate privacy control mechanisms that can be introduced to safeguard data protection, verify that remaining, residual risk to privacy principles will be acceptable and

7. Consider approaches, beyond the privacy controls in Step 6, that will enhance privacy for those deploying the specification or standard, such as limits on collection, limits for retention, rules for secure transfer, rules for limiting identification or obfuscation.

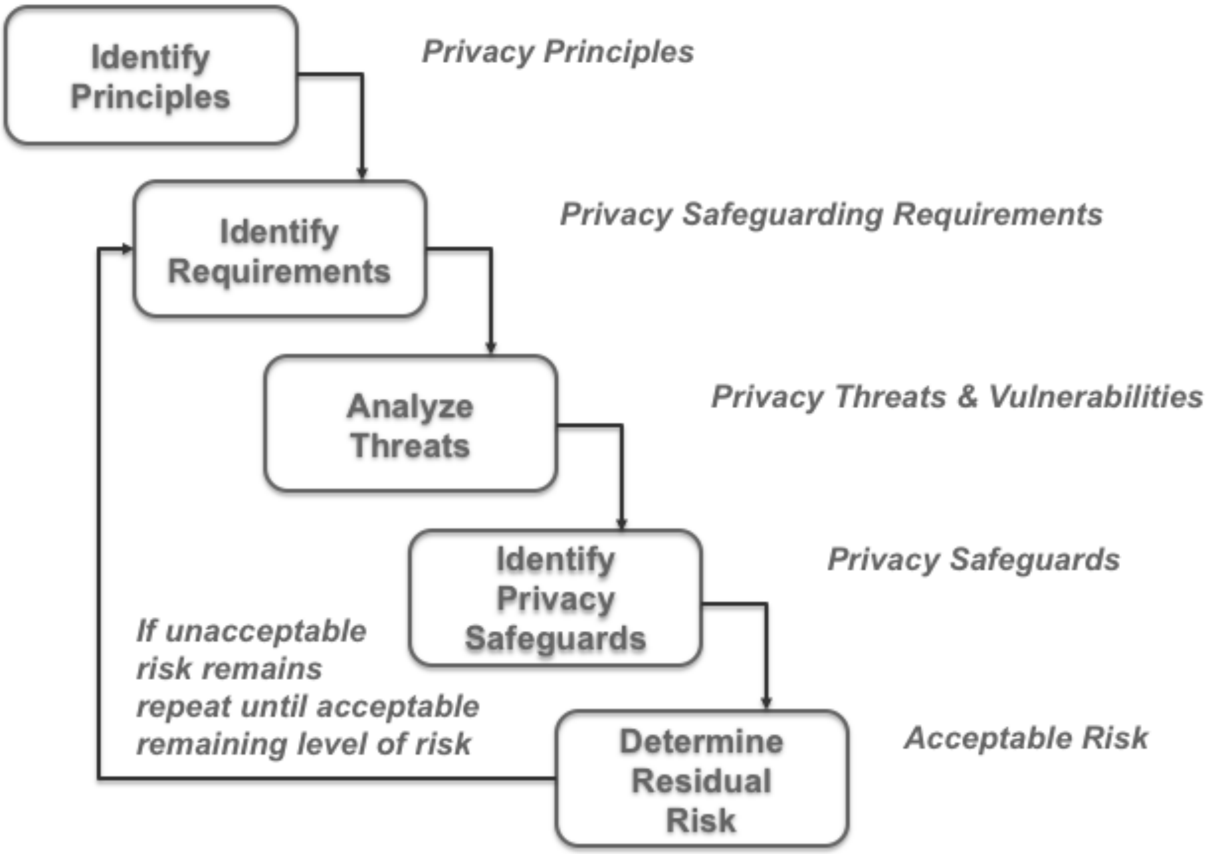
Identify Principles
Privacy Principles
Identify Requirements
Privacy Safeguarding Requirements
Analyze Threats
Privacy Threats & Vulnerabilities
Identify Privacy Safeguards
Privacy Safeguards
If unacceptable risk remains repeat until acceptable remaining level of risk
Determine Residual Risk
Acceptable Risk

Figure 3: Summary of SPA Process Intent

Step 1: ***Description*** - The SPA process is based on having a detailed understanding of the features and functions of the SUR. The description of the SUR generally includes an understanding of:

- Primary use cases for the features of the SUR,
- Internal interactors of the SUR. These include internal processes and data stores, as well as interfaces to external interactors,
- External interactors that the primary use cases of the SUR may either be dependent on or that the SUR maybe a dependent resource for. These include external processes and data stores,
- Identification of the data that flows between the internal interactors and external interactors, and
- Borders between the internal and external interactors that form a trust boundary.

Step 2: ***Data Flow*** - The old adage that “privacy impact comes with data” is true. Privacy impact is related to the processing of PII and the linkability of that PII to a data principal or individual (i.e., the individual’s identifiability). Detailing the data flow involved in a SUR is a key element to applying the SPA systematically. Ad hoc application of the SPA will result in incomplete application of safeguards and possibly lead to missing key vulnerabilities in the SUR.

Step 3: ***Data Analysis*** – Understanding the purpose and scope of the PII that is associated with the SUR is important in determining where unneeded data is being processed by the SUR or through the SUR by external interactors. One way to minimize the privacy impact of the SUR is to minimize the collection of PII in the first place and to limit the retention of that data for further processing. To assess this, the data flowing through the SUR needs to be identified and analyzed. There are a number of classification schemes that can be used to achieve this process step, but in general the analysis step should determine ***why*** the data is collected, ***what*** primary purpose there is for the processing of it, ***where*** it is being transferred or stored and ***how long*** it is being retained.

Step 4: ***Privacy Safeguarding Requirements*** – At this point in the SPA process, there should be sufficient information to evaluate the SUR to determine which privacy safeguarding requirements apply. This involves first understanding which privacy principles are applicable. ISO 29100/Privacy Framework [2] defines the privacy principles as:

1. Consent and choice,
2. Purpose legitimacy and specification,
3. Collection limitation,
4. Data minimization,
5. Use, retention and disclosure limitation,
6. Accuracy and quality,
7. Openness, transparency and notice,
8. Individual participation and access,
9. Accountability,
10. Information security, and
11. Privacy compliance.

The SUR should be reviewed to determine which of the ISO 29100 privacy principles are applicable. For each of the applicable privacy principles, identify appropriate privacy safeguarding requirements to be considered for the threat mitigation phase in Step 6.

Step 5: ***Threat Analysis*** – Threat Analysis is a step where the privacy principles, identified in Step 4, are analyzed to identify inherent vulnerabilities that a threat agent could utilize to create an unwanted incident with the technology being defined by the SUR that would threaten the privacy principle.

Step 6: ***Threat Mitigation*** – Mitigation of threats identified in Step 5 is necessary to create a robust privacy enhanced standard or specification. Threat mitigation involves selection of one or more privacy safeguarding requirement to thwart an identified threat.

Step 7: ***Deployment Considerations*** – Steps 1 to 6 when applied at an early stage in the creation of the standard or specification will assist in introducing more privacy enhancing design choices for the SUR. However, even when these steps are followed from New Work Item Proposal through Publication of the standard or specification, there are still considerations to take for the deployment of a published standard. In some cases, the organization deploying the SUR will be in the best position to consider introduction of privacy safeguards. This last step in the SPA process challenges the Editor or SC27/WG5 participants to consider what can be done during the implementation and deployment of the SUR to enhance the privacy of individuals who will be using ICT systems with the SUR embedded inside them. This final step in the analysis should take place prior to the SUR in question reaching the final development stage (e.g., FDIS).

6 Privacy Considerations Outline

The results of applying the SPA process is the creation of text within the SUR that outlines the privacy considerations that have been considered in the development of the standard or specification, as well as those that should be considered when deploying the standard or specification. This means that there should be a Privacy Considerations section in every SC27/WG5 standard and specification. In the case where it has been determined that the application of the SPA process is not warranted then this section would contain text such as:

> “This standard [or specification] does not define technology that will process Personally Identifiable Information (PII), nor will it create any link to PII.

> Furthermore, the standard [or specification] does not define technology that will be deployed in a network device and used by an individual."

However, in those cases where a SPA process has been determined to be warranted then this section needs to include text that:

- Catalogs the PII collected, its classification, instances of data storage, type of processing, instances of data transfer (against the privacy data lifecycle) from SPA Step 3;
- Identifies and list privacy threats from SPA Step 5;
- Identifies appropriate privacy safeguards/controls and context for mitigating identified threats from Step 6, and
- Identifies recommendations such as uses of privacy controls for organizations deploying the SUR that would additionally thwart the associated threats from Step 6.

And that text in this section would be in such a format as:

> "This standard [or specification] defines technology that will process Personally Identifiable Information (PII). The PII in this standard/specification includes the following categories of PII and its processing:
>
> - [Processing categories and PII category],
> - [Processing categories and PII category]…
>
> The PII processing defined by this standard/specification relates to the following privacy principles:
>
> - [privacy principle],
> - [privacy principle]…
>
> The organizations implementing this standard/specification should consider applying the following privacy requirements to mitigate risks to the above privacy principles:
>
> - [privacy requirement],
> - [privacy requirement]…"

7 References

[1] "Stages and resources for standards development", ISO, https://www.iso.org/stages-and-resources-for-standards-development.html.

[2] ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework