NORME INTERNATIONALE

ISO/IEC 29101

Deuxième édition
2018-11

Technologies de l'information — Techniques de sécurité — Architecture de référence pour la protection de la vie privée

Information technology — Security techniques — Privacy architecture framework

Numéro de référence
ISO/IEC 29101:2018(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes Internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 29101:2013), qui a fait l'objet d'une révision technique. La principale modification par rapport à l'édition précédente est que l'ancienne Annexe D a été supprimée.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Le présent document décrit une architecture de référence de haut niveau ainsi que les mesures associées visant à protéger la vie privée dans les systèmes de technologies de l'information et de la communication (TIC) qui stockent et traitent des données à caractère personnel (DCP).

L'architecture de référence pour la protection de la vie privée décrite dans le présent document:

— fournit une approche cohérente et de haut niveau pour la mise en œuvre de mesures de protection de la vie privée dans le cadre du traitement des DCP dans les systèmes TIC;

— fournit des recommandations pour la planification, la conception et l'élaboration d'architectures de systèmes TIC visant à protéger la vie privée des personnes concernées en contrôlant le traitement, l'accès et le transfert des informations personnelles identifiables; et

— indique comment les technologies renforçant la protection de la vie privée (PET) peuvent être utilisées comme mesures de protection de la vie privée.

Le présent document s'appuie sur le cadre de protection de la vie privée fourni par l'ISO/IEC 29100 dans le but d'aider une organisation à définir ses exigences en matière de protection de la vie privée, dans la mesure où elles concernent les DCP traitées par un système TIC. Dans certains pays, les exigences applicables en matière de protection de la vie privée sont considérées comme synonymes d'exigences de protection des données/de protection de la vie privée et font l'objet d'une législation sur la protection des données/la protection de la vie privée.

Technologies de l'information — Techniques de sécurité — Architecture de référence pour la protection de la vie privée

1 Domaine d'application

Le présent document définit une architecture de référence pour la protection de la vie privée qui:

— spécifie les enjeux des systèmes TIC ayant à traiter des DCP;

— énumère les éléments nécessaires à la mise en œuvre de tels systèmes; et

— fournit des vues de l'architecture contextualisant ces éléments.

Le présent document s'applique aux entités participant à la spécification, à la fourniture, à l'architecture, à la conception, aux essais, à la maintenance, à l'administration et à l'exploitation des systèmes TIC qui traitent des DCP.

Il se concentre principalement sur les systèmes TIC conçus pour interagir avec les personnes concernées.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements)

ISO/IEC 29100, *Technologies de l'information — Techniques de sécurité — Cadre privé*

ISO/IEC/IEEE 42010, *Ingénierie des systèmes et des logiciels — Description de l'architecture*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 29100 et l'ISO/IEC/IEEE 42010 s'appliquent.

4 Symboles et abréviations

Les abréviations suivantes s'appliquent au présent document.

DCP Données à caractère personnel

PET Technologie contribuant à la protection de la vie privée (Privacy Enhancing Technology)

TIC Technologies de l'information et de la communication

5 Vue d'ensemble de l'architecture de référence pour la protection de la vie privée

5.1 Éléments constitutifs de l'architecture

L'architecture de référence pour la protection de la vie privée présentée dans le présent document est destinée à servir de référence technique aux développeurs de systèmes TIC devant traiter des DCP. Le présent document ne fixe pas d'exigences en matière de politique de respect de la vie privée; il suppose qu'une telle politique est en place, que les exigences de protection de la vie privée ont été définies et que des mesures de protection appropriées ont été mises en œuvre au sein du système TIC.

Cette architecture de référence traite essentiellement de la protection des DCP. Étant donné qu'il s'agit en partie d'un objectif de sécurité, il convient que les systèmes TIC ayant à traiter des DCP suivent également les lignes directrices relatives à l'ingénierie de la sécurité de l'information. La présente architecture de référence répertorie certains éléments de sécurité de l'information, qui sont essentiels à la protection des DCP traitées au sein des systèmes TIC. L'architecture de référence présentée est basée sur le modèle utilisé dans l'ISO/IEC/IEEE 42010.

Les parties prenantes liées à ces enjeux concernent la protection de la vie privée et sont définies dans l'ISO/IEC 29100. Elles sont discutées plus en détail à l'Article 6.

Les enjeux de l'architecture de référence sont décrits à l'Article 7. Ils incluent les principes de protection de la vie privée de l'ISO/IEC 29100 et les exigences de protection de la vie privée spécifiques aux systèmes TIC.

L'architecture de référence est présentée comme suit:

a) les couches de l'architecture technique de référence décrites en 8.2 reflètent l'architecture du point de vue des éléments. Chaque couche regroupe des éléments ayant un objectif commun ou des fonctions similaires;

b) le modèle de déploiement exposé en 8.3 présente l'architecture de référence du point de vue d'un système TIC autonome. Chaque vue illustre un regroupement d'éléments en fonction de leur déploiement dans les systèmes TIC des parties prenantes; et

c) les vues du paragraphe 8.4 présentent l'architecture de référence d'un point de vue interactionnel. Ces vues illustrent la manière dont les éléments interagissent entre les systèmes TIC des différentes parties prenantes.

L'architecture de référence présente également des règles de correspondance entre les enjeux et les points de vue, établies sur la base de tables de correspondance.

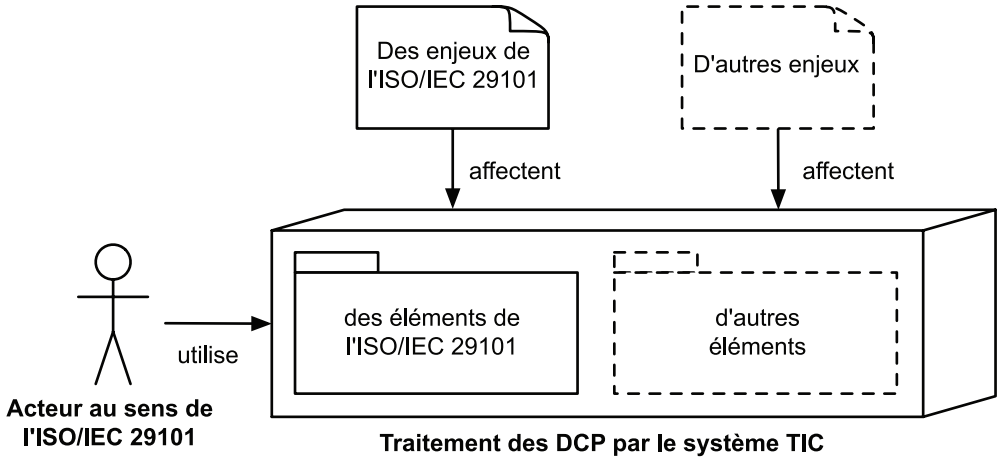

Figure 1 — Éléments de l'architecture de référence pour la protection de la vie privée dans leur contexte

La Figure 1 illustre la relation entre les éléments d'une architecture de référence pour la protection de la vie privée. L'élément central de l'architecture de référence est le système TIC intégré. Un acteur, au sens de l'ISO/IEC 29101, utilise un système TIC. La conception des systèmes TIC est affectée à la fois par les enjeux traités dans le présent document et, également, par d'autres enjeux. À titre d'exemples d'autres enjeux, on peut citer les exigences non fonctionnelles qui affectent les performances, l'accessibilité et la conception du système TIC, mais qui n'affectent pas le traitement fonctionnel des DCP. Ces autres enjeux n'entrent pas dans le cadre du présent document.

Le système TIC peut contenir des éléments de l'architecture de référence pour la protection de la vie privée détaillée dans le présent document ainsi que d'autres éléments. Ces éléments ne traitent pas les DCP, mais gèrent d'autres fonctionnalités du système TIC, comme l'accessibilité ou le recours à des interfaces utilisateur spécifiques. Ces éléments ne relèvent pas du domaine d'application du présent document.

5.2 Relation avec les systèmes de gestion

L'utilisation d'un système de gestion permet aux responsables de traitement des DCP et aux sous-traitants de DCP de répondre plus efficacement à leurs exigences de protection de la vie privée grâce à une approche structurée. Cette approche structurée permet également aux responsables de traitement des DCP et aux sous-traitants de DCP de mesurer les résultats et d'améliorer en permanence l'efficacité du système de gestion.

Un système de gestion efficace doit être aussi transparent que possible, tout en ayant un impact sur les personnes, les processus et la technologie. Il convient de l'intégrer au programme de contrôle interne et à la stratégie d'atténuation des risques d'une organisation. Sa mise en œuvre permet de se conformer plus facilement aux réglementations en matière de protection des données et de respect de la vie privée.

6 Acteurs et données à caractère personnel (DCP)

6.1 Vue d'ensemble

Les acteurs de l'architecture de référence ISO/IEC sont des parties prenantes en matière de protection de la vie privée, impliquées dans le traitement des DCP décrit dans l'ISO/IEC 29100. Il s'agit des acteurs suivants:

a) la personne concernée;

b) le responsable de traitement des DCP; et

c) le sous-traitant de DCP.

NOTE Le terme de «tiers» défini comme l'une des quatre catégories d'acteurs dans l'ISO/IEC 29100 est hors du domaine d'application de l'architecture de référence spécifiée dans le présent document.

Sur le plan du déploiement, l'architecture de référence est divisée en trois parties. Chaque partie s'applique au système TIC déployé du point de vue de chacun de ces acteurs.

La Figure 2 représente les systèmes TIC des acteurs ainsi que les flux de DCP entre ces systèmes. Elle illustre la division logique des fonctionnalités au niveau de l'architecture de référence décrite dans le présent document. Il ne s'agit pas d'une représentation de la structure physique, de l'organisation ou de la propriété du matériel des systèmes TIC.

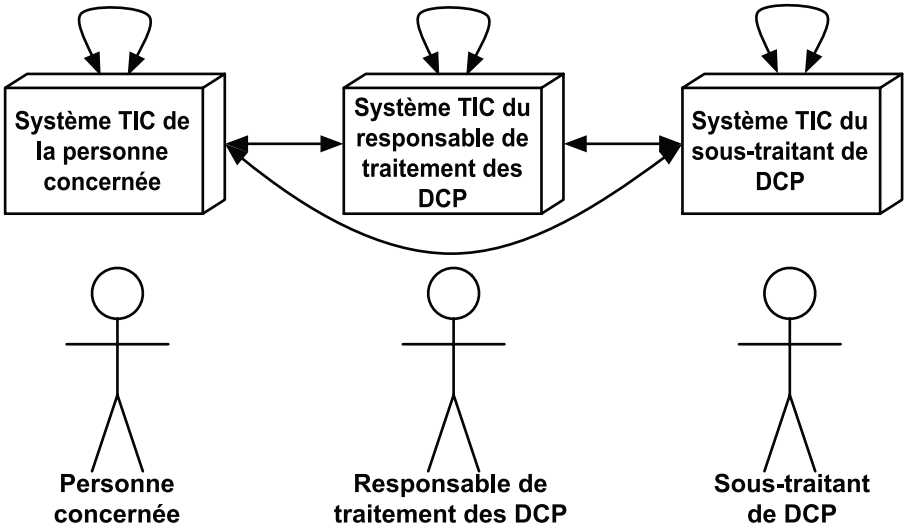

Figure 2 — Acteurs et leurs systèmes TIC au sens du présent document

Un acteur peut être responsable de la construction des systèmes TIC qu'il utilise, ou non. Par exemple, la personne concernée peut utiliser un système construit par le responsable de traitement des DCP, ou le système TIC de la personne concernée peut faire partie du système TIC du responsable de traitement des DCP. En outre, les fonctionnalités du système TIC de la personne concernée peuvent être réparties entre différents systèmes matériels TIC appartenant à la personne concernée et au responsable de traitement des DCP. De même, le responsable de traitement des DCP peut fournir le système TIC du sous-traitant de DCP. Les processus commerciaux ayant recours à des systèmes TIC utilisent un large éventail de modèles de communication et de modèles de confiance. L'architecture de référence présentée dans le présent document s'appuie sur une abstraction de ces modèles.

Si la personne concernée utilise un système TIC privé, les autres parties prenantes en matière de protection de la vie privée peuvent imposer des exigences à ce système TIC. Par exemple, le système TIC de la personne concernée peut devoir répondre à un minimum d'exigences de sécurité pour être autorisé à se connecter aux autres systèmes TIC. On peut également citer l'utilisation d'éléments de sécurité particuliers, tels que des jetons d'authentification matériels, certaines versions du système d'exploitation ou des versions spécifiques de navigateur Web.

Par exemple, dans les systèmes TIC utilisant des communications poste-à-poste (méthode, modèle ou technologie de communication permettant la communication entre des entités P2P sans serveur central), chaque application peut assumer les rôles des trois acteurs susmentionnés. Les informations sont à la fois envoyées et reçues par chaque poste, de sorte que chacun d'eux peut être responsable de traitement de DCP ou sous-traitant de DCP préalablement transmises par une autre partie jouant le rôle de personne concernée.

Dans les applications de réseaux sociaux, les DCP peuvent être traitées par toute personne ayant accès au profil d'autres personnes. Les applications de réseaux sociaux utilisant le Web permettent à tous les utilisateurs autorisés, et éventuellement anonymes, du service de traiter les DCP fournies par les personnes concernées, connectées au réseau social.

6.2 Phases du cycle de vie du traitement des DCP

6.2.1 Collecte

De nombreuses organisations collectent des informations sur des personnes concernées. Ces informations peuvent contenir des DCP.

Lorsqu'elles collectent des DCP, il convient que les organisations tiennent toujours compte des préférences relatives à la vie privée et des droits légaux de la personne concernée, ainsi que des

exigences de protection de la vie privée, telles que stipulées par la législation en vigueur. Des facteurs tels que le type de DCP, le consentement donné ou toute préférence exprimée en matière de respect de la vie privée, doivent être pris en compte à toutes les étapes du traitement. Il ne convient de collecter des DCP que si cela est nécessaire aux finalités déclarées.

Il convient d'associer une documentation aux DCP. On peut citer, sans s'y limiter, les exemples suivants:

a) balises logicielles indiquant la ou les finalités pour lesquelles les DCP peuvent être utilisées;

b) enregistrements décrivant la ou les finalités pour lesquelles les DCP peuvent être utilisées; et

c) enregistrements du consentement donné et de toute spécificité particulière qu'il convient de respecter (par exemple, il convient de chiffrer certaines catégories de DCP ou de les supprimer après un certain temps).

Il convient de mettre en œuvre des mesures de protection de la vie privée, chaque fois que des données sont identifiées comme DCP ou que des DCP sont caractérisées par des informations supplémentaires relatives à la personne concernée. Il est également important de préserver les balises pertinentes pour le traitement des DCP pendant les phases d'utilisation, de transfert, de stockage et d'élimination. Si des DCP stockées sont susceptibles d'avoir été modifiées, il convient d'en valider l'exactitude et la pertinence avant de les utiliser.

En outre, il convient que les processus de collecte des DCP soient conçus de manière à ne recueillir que les DCP nécessaires à la transaction concernée. Il convient que les organisations prennent des mesures visant à réduire au minimum la collecte non intentionnelle ou involontaire de DCP grâce à des systèmes de saisie de données (par exemple, formulaires d'applications Web permettant la saisie de toute information). Il convient de limiter l'introduction de DCP arbitraires en prévoyant un affichage contextuel des champs de saisie visant à réduire ou à éliminer les zones de formulaire Web où ces informations peuvent être entrées (par exemple, en supprimant les cases à cocher et les champs de texte libre inutiles). De même, il convient d'envisager l'utilisation de champs avec des entrées prédéfinies (par exemple, boîtes à liste et listes déroulantes) contenant des options autres que DCP. Lorsqu'il y a lieu d'implémenter des champs de texte libre, il convient que l'interface utilisateur prévoie:

a) des avertissements pour prévenir la personne concernée de ne pas saisir de DCP autres que celles qui sont explicitement demandées et autorisées ou exigées par la loi en vigueur;

b) une indication claire des champs dans lesquels des DCP doivent être saisies et une indication de la nature des DCP qu'il convient de saisir (par exemple, nom, adresse, informations médicales); et

c) une indication claire des champs où il convient de ne pas introduire de DCP.

6.2.2 Transfert

Le transfert, la diffusion ou la communication de DCP à des tiers signifie que les DCP ne sont plus sous le contrôle exclusif de la personne concernée. Le transfert est le terme généralement employé pour désigner la diffusion de DCP, depuis le responsable de traitement des DCP ou le sous-traitant de DCP vers d'autres responsables de traitement et sous-traitants de DCP. Si les DCP sont transférées, du responsable de traitement des DCP vers un autre acteur, le transfert est alors parfois appelé «divulgation».

Il convient que l'obligation de rendre compte et la responsabilité du transfert des DCP soient convenues et assumées par chaque partie impliquée dans le traitement des DCP. Il convient que cet accord soit mis par écrit lorsque la loi en vigueur l'exige. De plus, ces accords doivent être conformes à la législation sur la protection des données dans les domaines d'origine et de destination des transferts. Lorsque cela s'avère pertinent et approprié, ou lorsque la loi l'exige, il convient de notifier à la personne concernée qu'un transfert est en cours et de l'informer du contenu et de la finalité du transfert. En cas de litige entre la personne concernée et le responsable de traitement des DCP ou le sous-traitant de DCP, il convient de pouvoir accéder aux relevés des transferts de DCP pertinents pour aider à résoudre un tel litige.

Il convient d'éviter le transfert de DCP sensibles, sauf:

— s'il est nécessaire pour fournir un service que la personne concernée a demandé;

— s'il répond à une nécessité commerciale liée à la fourniture du service demandé; ou

— si la loi l'exige.

Certaines juridictions ont institué des lois qui exigent spécifiquement des accords contractuels formels incluant toutes les exigences de protection de la vie privée entre les parties concernées, lorsque des DCP sont transférées en dehors d'une juridiction ayant un niveau prescrit de protection de la vie privée. En cas de transferts transfrontaliers, il convient d'accorder une attention particulière aux mesures de protection des DCP transférées.

Il convient de mettre en place des mécanismes de protection appropriés lors du transfert de DCP. En cas de transfert numérique, il convient que les DCP soient transmises par un canal sécurisé ou sous forme chiffrée si la transmission se fait par un canal non sécurisé. Si les DCP sont transférées sur un support physique, il convient alors de les chiffrer. Si l'on utilise un chiffrement, il convient de ne pas stocker, ni transmettre la clé de chiffrement avec les DCP chiffrées.

6.2.3 Utilisation

L'utilisation de DCP désigne toute forme de traitement des DCP qui n'inclut pas la «collecte», le «transfert», le «stockage», l'« archivage » ou l'« élimination » de DCP. Les principes de protection de la vie privée décrits dans l'ISO/IEC 29100 (Cadre privé), ainsi que certaines lois sur la protection des données et le respect de la vie privée, peuvent limiter le traitement des DCP si ce traitement est incompatible avec les finalités spécifiées à l'origine. Il convient donc de ne traiter les DCP que dans le cadre des finalités déclarées pour lesquelles elles ont été collectées.

Si les DCP doivent être traitées à d'autres fins qui ne sont pas couvertes par la loi en vigueur, il convient d'obtenir le consentement de la personne concernée ou de son agent. Il convient de fournir à la personne concernée un moyen de contacter le responsable de traitement des DCP ou le sous-traitant de DCP au cas où la personne aurait des questions sur des activités nécessitant des éclaircissements.

Lorsqu'un tel traitement est jugé nécessaire, il convient d'obtenir le consentement de la personne concernée, à moins que la loi n'en dispose autrement. Il convient d'informer clairement les personnes concernées de l'utilisation spécifique de leurs DCP.

En outre, il convient d'appliquer des mécanismes de protection adaptés à l'utilisation des DCP, dans la mesure où une analyse approfondie des risques les juge nécessaire. Cela inclut l'utilisation de techniques d'anonymisation ou de pseudonymisation préalablement au traitement ainsi que le recours à des techniques de calcul sécurisées pendant le traitement.

6.2.4 Conservation

Lorsqu'il est nécessaire de stocker des DCP, il convient d'obtenir le consentement de la personne concernée, en tenant compte de toute mesure spécifique susceptible d'être exigée par la loi. Dans ces cas, il convient de ne conserver les DCP que pendant le temps nécessaire à la réalisation de la finalité professionnelle spécifique.

Il convient de stocker les DCP à l'aide de mesures de sécurité et de mécanismes appropriés afin d'empêcher toute action non autorisée, qu'il s'agisse d'accès, de modification, de destruction, de suppression ou de toute autre utilisation indue. De telles mesures de sécurité incluent, sans s'y limiter, le chiffrement, le secret réparti, la pseudonymisation et l'anonymisation.

Les DCP archivées doivent faire l'objet d'une attention particulière. Les principes de protection de la vie privée stipulent qu'il convient que les DCP ne soient conservées que le temps nécessaire à la réalisation des finalités déclarées, puis qu'elles soient détruites par des moyens sûrs ou anonymisées. Toutefois, si le responsable de traitement des DCP ou le sous-traitant de DCP est contraint, du fait de la loi en vigueur, de conserver les DCP au-delà de l'expiration des autres finalités, il convient de verrouiller les

DCP (c'est-à-dire de les archiver et de les protéger par un mécanisme de contrôle d'accès pour éviter toute utilisation ultérieure). Il convient avant tout, lors de l'archivage des DCP, de s'assurer que les mécanismes appropriés de protection des données sont en place, y compris les solutions de gestion des accès qui ne permettent l'accès aux DCP archivées qu'aux utilisateurs autorisés.

Il convient que le responsable de traitement des DCP mette en place des mesures de sécurité dans les systèmes de stockage afin de pouvoir éliminer les DCP lorsqu'elles expirent ou lorsque la finalité du stockage ou du traitement des DCP ne se justifie plus.

6.2.5 Élimination

Au cours de la dernière étape du cycle de vie du traitement des DCP, les DCP sont supprimées, anonymisées, détruites, renvoyées ou éliminées d'une autre manière. Il est possible d'empêcher toute utilisation non autorisée de certaines DCP dans des relevés de DCP en les marquant pour élimination. Il convient de noter que la suppression de DCP ne signifie pas nécessairement que celles-ci sont définitivement éliminées, car les DCP supprimées dans des systèmes TIC peuvent souvent être récupérées. Bien que cela puisse sembler évident dans le traitement des DCP, les procédures d'élimination des DCP ne satisfont pas toujours aux exigences de protection de la vie privée. Il convient que les spécifications fournies par la personne concernée (telles que la finalité d'utilisation) ou les exigences spécifiées par la législation (telles que la date d'expiration de DCP spécifiques) soient prises en compte avant que des DCP ne soient éliminées.

7 Enjeux

7.1 Vue d'ensemble

Un enjeu, tel que défini dans l'ISO/IEC/IEEE 42010, est un intérêt au sein d'un système, qui est pertinent pour une ou plusieurs de ses parties prenantes. L'architecture de référence pour la protection de la vie privée exposée dans le présent document est essentiellement axée sur les enjeux des parties prenantes en matière de protection de la vie privée, liés au traitement des DCP. Les enjeux du présent document comprennent les principes de protection de la vie privée de l'ISO/IEC 29100 ainsi que toute exigence de protection de la vie privée dérivée de ces principes et conforme à ceux-ci.

Il convient de déterminer les exigences de protection de la vie privée en suivant un processus de gestion des risques d'atteinte à la vie privée, conforme au processus décrit dans l'ISO/IEC 29100:2011, 4.5. Il convient que toute personne ou organisation qui conçoit un système TIC manipulant des DCP suive ce processus. Il convient que toutes les exigences identifiées en matière de protection de la vie privée soient conformes à la législation applicable en la matière.

7.2 Les principes de protection de la vie privée de l'ISO/IEC 29100

Le responsable de traitement des DCP est chargé, pour l'ensemble de l'organisation, de la protection des DCP et de la gestion loyale et licite de celles-ci à tout moment, ainsi que du traitement des DCP délégué aux sous-traitants de DCP.

Le responsable de traitement des DCP a la charge, en dernier ressort, de la mise en œuvre des mesures de protection de la vie privée au sein d'un système TIC. Les mesures de protection de la vie privée visent à garantir que les exigences de protection de la vie privée définies pour une personne concernée, une transaction ou un scénario spécifique sont prises en compte et strictement respectées. Il convient d'apporter la preuve de la mise en œuvre des mesures de protection de la vie privée, en les documentant correctement et en fournissant des documents d'audit qui vérifient que ces mesures de sécurité existent, qu'elles ont été correctement mises en œuvre et qu'elles fonctionnent convenablement. Pour finir, il convient que le responsable de traitement des DCP accepte et adhère aux principes de protection de la vie privée décrits dans l'ISO/IEC 29100, à savoir:

a) consentement et choix;

b) licéité et spécification de la finalité;

c) limitation de la collecte;

d) minimisation des données;

e) limitation de l'utilisation, de la conservation et de la divulgation;

f) exactitude et qualité;

g) ouverture, transparence et information;

h) participation et accès individuels;

i) responsabilité;

j) sécurité de l'information; et

k) conformité aux règles de protection de la vie privée.

7.3 Exigences de protection de la vie privée

Il convient que les systèmes TIC mettent en œuvre des mesures de protection de la vie privée en tant qu'élément principal de chaque phase du cycle de vie du traitement des DCP. Les exigences de protection de la vie privée permettent au concepteur du système TIC de concrétiser le lien entre les principes de protection de la vie privée et les éléments architecturaux présentés à l'Article 8.

Afin de mettre en œuvre des mesures efficaces de protection de la vie privée dans un système TIC, il convient de créer des flux de traitement décrivant le traitement des DCP. Les diagrammes de flux de traitement des DCP constituent une représentation graphique du «flux» de DCP circulant au sein du système TIC et entre les différents acteurs. Par exemple, si un acteur transfère des DCP à d'autres acteurs (par exemple, des sous-traitants de DCP), il convient d'inclure ces transferts de DCP dans le diagramme de flux de traitement des DCP.

Un diagramme de flux de traitement des DCP peut également être représenté sous la forme d'un tableau de flux de DCP. Ce diagramme ou tableau suit la collecte, le transfert, l'utilisation, le stockage ou l'élimination des DCP et contient des informations telles que le type de DCP, la personne qui a collecté les DCP, la finalité du traitement, la personne à qui les DCP vont être transférées, l'obtention du consentement de la personne concernée, la période de conservation et l'endroit où les DCP sont stockées, ainsi que le niveau de risque d'atteinte à la vie privée, qui en résulte. Les informations sur les flux de traitement des DCP sont un élément du processus de gestion des risques d'atteinte à la vie privée, qui génère les exigences de protection de la vie privée.

Une fois l'analyse des exigences d'un système TIC terminée, il convient que les développeurs fassent correspondre les exigences de protection de la vie privée du système TIC avec la liste des enjeux du présent document. Il convient alors que les exigences de protection de la vie privée soient utilisées pour choisir les éléments architecturaux satisfaisant aux dites exigences.

L'Annexe A contient un exemple de liste d'enjeux et illustre comment lier ces enjeux aux principes de protection de la vie privée de l'ISO/IEC 29100 ainsi qu'aux éléments architecturaux du présent document.

8 Vues de l'architecture

8.1 Généralités

Le présent article est structuré autour de trois points de vue architecturaux. Tout d'abord, la vue Éléments décrit en détail les éléments du système TIC et les sépare en couches, selon leur fonctionnalité. Chaque couche regroupe des éléments qui contribuent au traitement correct des DCP. Des recommandations de mise en œuvre limitée sont fournies pour chaque élément. Des recommandations spécifiques aux acteurs sont fournies, le cas échéant. Cette vue est utile pour comprendre les blocs constitutifs de l'architecture de référence pour la protection de la vie privée.

Des tableaux présentant des exemples de relations types entre les principes de protection de la vie privée de l'ISO/IEC 29100 et les éléments de l'architecture sont fournis dans la vue Éléments. De tels tableaux de correspondance sont utiles pour comprendre comment un système TIC adhère aux principes de protection de la vie privée de l'ISO/IEC 29100. Des tableaux similaires peuvent être utilisés à titre d'exemples et mis à jour lors de la conception du système pour décrire comment un système TIC particulier adhère aux principes de protection de la vie privée de l'ISO/IEC 29100.

La vue Acteurs considère les éléments décrits dans la vue Éléments, du point de vue du système TIC d'un acteur individuel. Cette vue est utile pour la conception de l'architecture d'un système TIC particulier. La vue Interactions considère les éléments d'un point de vue du déploiement. Cette vue permet de comprendre comment les éléments des systèmes TIC des différents acteurs interagissent les uns avec les autres.

8.2 Vue Éléments

8.2.1 Généralités

La vue Éléments sert à décrire les éléments d'un système TIC qui interviennent dans le traitement des DCP.

Il convient que le choix des éléments soit guidé par les exigences appropriées de protection de la vie privée. Il convient que le développeur du système TIC destiné à un ou plusieurs acteurs spécifiques (voir Figure 2) utilise la vue Éléments pour déterminer les éléments à inclure dans l'architecture du système qu'il élabore. Il convient que cette architecture soit basée sur les exigences de protection de la vie privée établies à l'aide des recommandations de l'Article 7. Il est à noter que tous les éléments décrits dans le présent document ne conviennent pas nécessairement à tout système TIC.

La vue Éléments se décompose en trois couches. Chaque couche correspond à un groupe logique d'éléments qui contribuent à un objectif spécifique dans le traitement des DCP. Les éléments de la couche Paramètres de protection de la vie privée gèrent les métadonnées relatives au traitement des DCP, y compris, entre autres, l'échange d'informations sur la finalité du traitement, le consentement et les préférences de la personne concernée. Les éléments de la couche Gestion des identités et des accès doivent pouvoir garantir que des informations d'identité appropriées sont utilisées dans le traitement des DCP et que l'accès aux DCP est contrôlé conformément aux exigences de protection de la vie privée. Pour finir, les éléments de la couche DCP exécutent diverses tâches de traitement des DCP.

L'architecture de référence est conçue en partant du principe que tous les éléments interagissent avec plusieurs autres éléments. Toutefois, afin de préserver le caractère général et la clarté du document, les possibilités d'interactions entre les éléments n'ont pas été représentées.

Certains des éléments de l'architecture de référence sont des technologies contribuant à la protection de la vie privée (appelées technologies PET). Cette sélection de technologies PET n'est pas exhaustive. Il en existe d'autres qui ne sont pas décrites dans le présent document et c'est au développeur du système TIC qu'il incombe de choisir les technologies PET appropriées et de les adapter à l'architecture de référence.

L'Annexe B donne un exemple d'architecture de système TIC appliquant des technologies PET pour garantir un traitement sûr des DCP. L'Annexe C donne un exemple de la manière d'utiliser des données d'identification basées sur des attributs pour élaborer un système TIC qui assure la gestion des identités pseudonymes et du contrôle d'accès.

Les paragraphes suivants décrivent les couches, les éléments qui les composent et les acteurs qui interagissent avec ces éléments. Chaque élément fait l'objet d'une description générale, suivie de lignes directrices spécifiques aux acteurs. Pour certains éléments, il n'est donné aucune recommandation spécifique aux systèmes TIC d'un acteur particulier, car le comportement de l'élément est similaire dans les systèmes TIC de tous les acteurs.