

ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Duben 2016**

Informační technologie - Bezpečnostní techniky -
Rámec architektury soukromí

ČSN
ISO/IEC 29101
36 9708

Information technology - Security techniques - Privacy architecture framework

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

Tato norma je českou verzí mezinárodní normy ISO/IEC 29101:2013. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 29101:2013. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 29100:2011 zavedena v ČSN ISO/IEC 29100:2015 (36 9705) Informační technologie - Bezpečnostní techniky - Rámec soukromí

ISO/IEC/IEEE 42010:2011 dosud nezavedena

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - ISO/IEC 29101
Rámec architektury soukromí První vydání
2013-10-15

ICS 35.040

Obsah

Předmluva	6
Úvod	7
1 Předmět normy	8
2 Citované dokumenty	8
3 Termíny a definice	8
4 Symboly a zkrácené termíny	8
5 Přehled rámce architektury soukromí	8
5.1 Prvky rámce	8
5.2 Vztah se systémy řízení	9
6 Aktéři a PII	9
6.1 Přehled	9
6.2 Fáze životního cyklu zpracování PII	10
6.2.1 Shromažďování	10
6.2.2 Přenos	11
6.2.3 Použití	11
6.2.4 Uložení	12
6.2.5 Likvidace	12
7 Problémy	12
7.1 Přehled	12
7.2 Principy soukromí z ISO/IEC 29100	12
7.3 Požadavky na ochranu soukromí	13
8 Architektonický pohled	13
8.1 Úvod	13
8.2 Pohled komponenty	13
8.2.1 Vrstva nastavení soukromí	14
8.2.2 Vrstva řízení identity a řízení přístupu	17
8.2.3 Vrstva PII	18

8.3 Pohled aktéra 23

8.3.1 Systém ICT subjektu PII 24

8.3.2 Systém ICT dohlázeitele PII 24

8.3.3 Systém ICT zpracovatele PII 25

8.4 Pohled interakce 26

8.4.1 Vrstva nastavení soukromí 27

Strana

8.4.2 Vrstva řízení identity a přístupu 27

8.4.3 Vrstva PII 28

Příloha A (informativní) Příklady problémů systému ICT souvisících s PII 29

A.1 Úvod 29

A.2 Obdržení a komunikování souhlasu 29

A.3 Komunikování účelu shromažďování PII 29

A.4 Bezpečné zpracování PII 30

A.5 Klasifikace a řízení PII 30

A.6 Analyzování a audit operací PII 30

A.7 Archivování a likvidace PII 31

A.8 Vztah s principy soukromí 33

Příloha B (informativní) Systém agregace PII s bezpečným výpočtem 34

B.1 Úvod 34

B.2 Účel, aktéři a nasazení 34

B.3 Architektura pro aplikace vstupu PII 35

B.4 Architektura pro aplikaci řízení studie 36

B.5 Architektura pro aplikaci bezpečné analýzy PII 37

B.6 Závěrečné shrnutí 38

Příloha C (informativní) K soukromí přátelský pseudonymní systém pro řízení identity a přístupu 40

C.1 Úvod 40

C.2 Účel, aktéři a nasazení 40

C.3 Architektura systému ICT Vydavatele univerzitních průkazných informací 41

C.4 Architektura systému ICT studenta 42

C.5 Architektura Aplikace hodnocení kurzů 43

C.6 Závěrečné shrnutí 44

Příloha D (informativní) Spojitost principů soukromí a opatření bezpečnosti informací 46

Obrázky

Obrázek 1 - Prvky rámce architektury soukromí v kontextu 9

Obrázek 2 - Aktéři a jejich systémy ICT podle ISO/IEC 29101 10

Obrázek 3 - Architektura systému ICT subjektu PII 24

Obrázek 4 - Architektura systému ICT dohlážitelce PII 25

Obrázek 5 - Architektura systému ICT zpracovatele PII 26

Obrázek 6 - Nasazení komponent ve vrstvě nastavení soukromí 27

Obrázek 7 - Nasazení komponent ve vrstvě řízení identity a přístupu 27

Obrázek 8 - Nasazení komponent ve vrstvě PII 28

Obrázek B.1 - Nasazení bezpečného výpočetního systému 35

Obrázek B.2 - Architektura vstupu PII do systému ICT 35

Obrázek B.3 - Architektura systému ICT koordinátora studie 36

Obrázek B.4 - Architektura pro aplikaci bezpečné analýzy dat 37

Obrázek C.1 - Přehled architektury - aktéři a jejich interakce 41

Obrázek C.2 - Architektura systému ICT Vydavatele univerzitních průkazných informací 41

Obrázek C.3 - Architektura systému ICT studenta 42

Obrázek C.4 - Architektura Aplikace hodnocení kurzu 44

Strana

Tabulky

Tabulka 1 - Příklad vztahu mezi principy soukromí a komponentami ve vrstvě nastavení soukromí 16

Tabulka 2 - Příklad vztahu mezi principy soukromí a komponentami ve vrstvě řízení identity a přístupu 18

Tabulka 3 - Příklad vztahu mezi principy soukromí a komponentami ve vrstvě PII 23

Tabulka A.1 – Příklady vztahu mezi problémy a komponentami ve vrstvě nastavení soukromí 31

Tabulka A.2 – Příklady vztahu mezi problémy a komponentami ve vrstvě řízení identity a přístupu 31

Tabulka A.3 – Příklady vztahu mezi problémy a komponentami ve vrstvě PII 32

Tabulka A.4 – Příklady vztahu mezi principy soukromí a obecnými problémy 33

Tabulka D.1 – Principy soukromí a odpovídající opatření bezpečnosti informací 46

DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2013

Veškerá práva vyhrazena. Není-li specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakémkoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně pořizování fotokopií nebo zveřejnění na internetu nebo intranetu, bez předchozího písemného svolení. O písemné svolení lze požádat buď přímo ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikování jakéhokoliv nebo všech patentových práv.

ISO/IEC 29101 vypracovala společná technická komise ISO/IEC JTC1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Úvod

Tato mezinárodní norma popisuje obecný rámec architektury a připojená opatření pro ochranu soukromí v systémech informační a komunikační technologie (ICT), které ukládají a zpracovávají osobně identifikovatelné informace (PII).

Rámec architektury soukromí popsany v této mezinárodní normě

- poskytuje konzistentní, obecný přístup k implementaci opatření na ochranu soukromí pro zpracování PII v systémech ICT;
- poskytuje návod pro plánování, navrhování a konstrukce architektury systémů ICT, které zajišťují ochranu soukromí subjektů PII řízením zpracování osobně identifikovatelných informací, přístupu k nim a jejich přenosu; a
- ukazuje, jak technologie zlepšující soukromí (PET) mohou být použity k opatřením na ochranu soukromí.

Tato mezinárodní norma je postavena na rámci soukromí, poskytnutém v ISO/IEC 29100, aby pomohla organizaci definovat její požadavky na ochranu soukromí, vztahující se k PII zpracovávanými jakýmkoliv systémem ICT. V některých zemích jsou požadavky na ochranu soukromí chápány jako synonymní s požadavky na ochranu dat/soukromí a jsou předmětem legislativy na ochranu dat/soukromí.

Tato mezinárodní norma se zaměřuje na systémy ICT, které jsou navrženy k interakci se subjekty PII.

1 Předmět normy

Tato mezinárodní norma definuje rámec architektury soukromí, který:

- specifikuje problémy systémů ICT, které zpracovávají PII;
- uvádí komponenty pro implementaci takových systémů; a
- poskytuje architektonický pohled, který dává tyto komponenty do kontextu.

Tato mezinárodní norma je aplikovatelná na entity zapojené do specifikování, pořizování, architektury, navrhování, testování, udržování, administrování a provozování systémů ICT zpracovávajících PII.

Zaměřuje se především na systémy ICT, které jsou navrženy pro vzájemnou interakci se subjekty PII.

Konec náhledu - text dále pokračuje v placené verzi ČSN.