

2020

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 29101:2018. Překlad byl zajištěn Českou
agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 29101:2018. It was translated
by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 29101 (36 9708) z dubna 2016.

Národní předmluva

Změny proti předchozí normě

Toto druhé vydání zrušuje a nahrazuje první vydání, které bylo technicky zrevidováno. Hlavní
změnou je vypuštění přílohy D.

Informace o citovaných dokumentech

ISO/IEC 29100 zavedena v ČSN ISO/IEC 29100 (36 9705) Informační technologie – Bezpečnostní
techniky – Rámec soukromí

ISO/IEC/IEEE 42010 dosud nezavedena

Vysvětlivky k textu převzaté normy

Pro účely této normy je anglický termín „credentials“ přeložen jako „průkazní informace“.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

ICS 35.030

Obsah

	Strana
Předmluva.....	
..... 5	
Úvod.....	
..... 6	
1..... Předmět	
normy.....	
..... 7	
2..... Citované	
dokumenty.....	
..... 7	
3..... Termíny	
a definice.....	
..... 7	
4..... Symboly	
a zkratky.....	
..... 7	
5..... Přehled rámce architektury	
soukromí.....	7
5.1..... Prvky	
rámce.....	
..... 7	
5.2..... Vztah k systémům	
řízení.....	
..... 8	
6..... Aktéři	
a PII.....	
..... 8	
6.1.....	
Přehled.....	

.....	8
6.2..... Fáze životního cyklu zpracování	
PII.....	9
6.2.1...	
Shromažďování.....	
.....	9
6.2.2...	
Přenos.....	
.....	10
6.2.3...	
Použití.....	
.....	10
6.2.4...	
Uložení.....	
.....	11
6.2.5...	
Likvidace.....	
.....	11
7.....	
Problémy.....	
.....	11
7.1.....	
Přehled.....	
.....	11
7.2..... Principy soukromí	
z ISO/IEC 29100.....	
....	11
7.3..... Požadavky na ochranu	
soukromí.....	
	12
8..... Architektonické	
pohledy.....	
.....	12
8.1.....	
Obecně.....	
.....	12
8.2..... Pohled	
komponenty.....	
.....	12

8.2.1...	
Obecně.....	
.....	12
8.2.2... Vrstva nastavení	
soukromí.....	
.....	13
8.2.3... Vrstva řízení identity a řízení	
přístupu.....	16
8.2.4... Vrstva	
PII.....	
.....	17
8.3..... Pohled	
aktéra.....	
.....	22
8.3.1...	
Obecně.....	
.....	22
8.3.2... Systém ICT subjektu	
PII.....	
..	22
8.3.3... Systém ICT dohlázele	
PII.....	
22	
8.3.4... Systém ICT zpracovatele	
PII.....	23

8.4.....	Pohled	
interakce.....		
.....	24	
8.4.1...		
Obecně.....		
.....	24	
8.4.2...	Vrstva nastavení	
soukromí.....		
.....	24	
8.4.3...	Vrstva řízení identity	
a přístupu.....		
..	24	
8.4.4...	Vrstva	
PII.....		
.....	25	
Příloha A	(informativní) Příklady problémů systému ICT souvisících	
s PII.....		27
Příloha B	(informativní) Systém shromažďování PII bezpečným	
výpočtem.....		31
Příloha C	(informativní) K soukromí přátelský pseudonymní systém pro řízení identity	
a přístupu.....		37



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2018

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopíí nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Fax: + 41 22 749 09 47

Email: copyright@iso.org

Website: www.iso.org

Publikováno ve Švýcarsku

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 oborech společného zájmu. 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.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů. Tento dokument byl vypracováván v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz www.iso.org/directives).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržných ISO (viz www.iso.org/patents).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamena schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT) viz www.iso.org/iso/foreword.html.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *IT Bezpečnostní techniky*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 29101:2013), které bylo technicky zrevidováno. Hlavní změnou proti předchozímu vydání je vypuštění přílohy D.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu by měly být směřovány na národní normalizační orgán uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html.

Úvod

Tento dokument popisuje obecný rámec architektury a přiložená opatření pro ochranu soukromí v systémech informační a komunikační technologie (ICT), které ukládají a zpracovávají osobně identifikovatelné informace (PII).

Rámec architektury soukromí popsany v tomto dokumentu:

- poskytuje konzistentní, obecný přístup k implementaci opatření na ochranu soukromí pro zpracování PII v systémech ICT;
- poskytuje návod pro plánování, navrhování a konstrukce architektur 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.

Tento dokument vychází z rámce soukromí, poskytnutém v ISO/IEC 29100, aby pomohl 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.

1 Předmět normy

Tento dokument 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.

Tento dokument je aplikovatelný na entity účastníci se 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.