ČESKÁ TECHNICKÁ NORMA

ICS 35.240.80 **Říjen 2010**

Zdravotnická informatika – Bezpečná identifikace uživatele pro zdravotní péči – Správa a bezpečnost autentizace heslem

ČSN
EN 12251
98 2012

Health informatics – Secure User Identification for Health Care –
Management and Security of Authentication by Passwords

Informatique de santé – Sécurité de l'identification de l'utilisateur des soins de santé –

Gestion et sécurité de l'authentification des mots de passe

Medizinische Informatik – Sichere Nutzeridentifikation im Gesundheitswesen –

Management und Sicherheit für die Authentifizierung durch Passwörter

Tato norma je českou verzí evropské normy EN 12251:2004. 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 European Standard EN 12251:2004. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN 12251 (98 2012) z března 2005.

Národní předmluva

Vypracování normy

Zpracovatel: INFO 7, IČ 44266154, Ing. Jaroslav Ošlejšek

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

EVROPSKÁ NORMA EN 12251
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM Srpen 2004

ICS 35.240.80

Zdravotnická informatika –
Bezpečná identifikace uživatele pro zdravotní péči –
Správa a bezpečnost autentizace heslem

Health informatics – Secure User Identification for Health Care –
Management and Security of Authentication by Passwords

Informatique de santé – Sécurité de l'identification de l'utilisateur des soins de santé – Gestion et sécurité de l'authentification des mots de passe

Medizinische Informatik – Sichere Nutzeridentifikation im Gesundheitswesen – Management und Sicherheit für die Authentifizierung durch Passwörter

Tato evropská norma byla schválena CEN 2004-06-21.

Členové CEN jsou povinni splnit Vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se musí této evropské normě bez jakýchkoliv modifikací dát status národní normy. Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru nebo u kteréhokoliv člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, České republiky, Dánska, Estonska, Finska, Francie,
Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

CEN

Evropský výbor pro normalizaci
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Řídicí centrum: rue de Stassart 36, B-1050 Brusel

Předmluva

Tento dokument (EN 12251:2004) byl připraven technickou komisí ISO/TC 215 „Zdravotnická informatika“ ve spolupráci s technickou komisí CEN/TC 251 „Zdravotnická informatika“ jejímž sekretariátem je SIS.

Této evropské normě je nutno nejpozději do února 2005 dát status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do února 2005.

Tento dokument nahrazuje ENV 12251:2000.

Tento dokument je určen ke zlepšení autentizace jednotlivých uživatelů IT systémů zdravotní péče, posílení automatizovaných softwarových postupů spojených se správou uživatelských identifikátorů a hesel, aniž by se

vyhledávala další hardwarová zařízení.

Ačkoli se používají hesla, a potřeba větší bezpečnosti v tomto ohledu není v žádném případě pro oblast zdravotnictví specifická, je zřejmé, že způsob, jak se v této oblasti systémy používají často jako přímá podpora péče o pacienta a manipulace s velmi citlivými informacemi, naléhavě volá po kvalitním řešení. Nicméně, metody uvedené v tomto dokumentu mohou být případně použity v jiných odvětvích a i podle uvážení uživatelů.

Podle Vnitřních předpisů CEN/CENELEC jsou tuto evropskou normu povinny zavést národní normalizační
organizace následujících zemí: Belgie, České republiky, Dánska, Estonska, Finska, Francie, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Řecka, Slovenska, Slovinska, Spojeného království, Španělska, Švédska a Švýcarska.

Obsah

Strana

Úvod

Systémy informačních technologií (IT) v prostředí zdravotní péče jsou užívány ve stále více choulostivých a kritických okolnostech. Pro ulehčení kontroly bezpečného přístupu k informačnímu systému v rámci systému IT, je nezbytné zavést jedinečnou identitu všech uživatelů usilujících o přístup. Dále je nutné mít jistotu, že uživatel je opravdu ten nebo ona, kdo tvrdí že je, proto je nezbytné mít bezpečný prostředek k ověření uplatňované identity. Použití hesel je pro každého uživatele důvěrné a je konstruováno takovým způsobem, aby ostatní nemohli snadno kompromitovat tuto důvěrnou autentizační informaci, která je nejběžnějším prostředkem autentizace v současných počítačových systémech a bude tomu tak ještě po nějaký čas. Tento dokument může ulehčit širší proces správy bezpečnosti.

Tradiční hesla mají několik nedostatků. Některé z nich jsou:

- mohou být snadno sdílena mezi několika uživateli;
- použití nechráněné síťové technologie je snadným cílem pro tajné získávání informací;
- mohou být nesnadno zapamatovatelná, jestliže jsou vybraná tak, aby byla bezpečná.

Jiné technologie, jako jsou čipové karty a biometrika, které poskytují bezpečnější prostředky autentizace, se zavádějí do užívání a budou postupně nahrazovat použití hesel. Nicméně v současné době je důležité podporovat ve zdravotních informačních systémech co nejbezpečnější použití hesel. To je hlavním cílem tohoto dokumentu.

1 Předmět normy

Tento dokument byl navržen proto, aby podpořil zdokonalení autentizace jednotlivých uživatelům IT systémů zdravotní péče posilováním automatických softwarových procedur spojených se správou identifikací uživatele a hesel, bez pomoci dalších hardwarových zařízení.

Tento dokument se dá použít ve všech informačních systémech (dále jen systémech) v rámci prostředí zdravotní péče, které manipulují nebo ukládají citlivé, osobu identifikující zdravotní informace pomocí hesel jako jediného způsobu autentizace zadaného identifikátoru uživatele, tj.

ověřením uživatelem poskytnuté identity. Systémy, které spadají do působnosti tohoto dokumentu, zahrnují například elektronické systémy záznamů o pacientovi, administrativní a laboratorní systémy, které obsahují zdravotní informace o osobě.

Tento dokument se nevztahuje na systémy, které jsou vně prostředí zdravotní péče. Nedá se použít na systémy v rámci prostředí zdravotní péče, které používají jiné prostředky identifikace a autentizace jako jsou čipové karty, biometrické metody nebo jiná technická zařízení.