ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA Júl 2021

STN	**Informačné technológie Bezpečnostné metódy Požiadavky na čiastočne anonymné a čiastočne nezrušiteľné overenie totožnosti**	**STN ISO/IEC 29191** 97 4137

Information technology
Security techniques
Requirements for partially anonymous, partially unlinkable authentication

Technologies de l'information
Techniques de sécurité
Exigences pour l'authentification partiellement anonyme, partiellement non reliable

Informationstechnologie
Sicherheitstechniken
Anforderungen für eine teilweise anonyme, teilweise nicht verknüpfbare Authentifizierung

Táto norma obsahuje anglickú verziu ISO/IEC 29191: 2012.

This standard includes the English version of ISO/IEC 29191: 2012.

obsahuje farebné strany

132935

Anotácia

Pri mnohých druhoch transakcií by entita radšej zostala anonymná a nezistiteľná, čo znamená, že keď sa vykonávajú dve transakcie, je ťažké rozlíšiť, či transakcie vykonáva ten istý používateľ alebo dvaja rôzni používatelia. Za určitých okolností však existujú legitímne dôvody umožňujúce následnú opätovnú identifikáciu (napr. v záujme zodpovednosti). Pojem „čiastočne anonymný, čiastočne nezistiteľný“ znamená, že apriórne určená entita a iba táto určená entita môže identifikovať autentifikovanú entitu.

Táto medzinárodná norma poskytuje rámec a ustanovuje požiadavky na čiastočne anonymné a čiastočne nezistiteľné overenie.

Národný predhovor

Normatívne referenčné dokumenty

V tomto dokumente nie sú uvedené žiadne normatívne referenčné dokumenty.

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC should not be held responsible for identifying any or all such patent rights.

ISO/IEC 29191 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, subcommittee SC 27, *IT Security techniques*.

Introduction

The current state of the art for entity authentication requires the revelation of the identifiable information of an entity being authenticated. In many types of transactions, the entity would prefer to remain anonymous and unlinkable, which means that when two transactions are performed, it is difficult to distinguish whether the transactions are performed by the same user or two different users. However, in some circumstances there are legitimate reasons to enable subsequent reidentification (e.g., the interest of accountability). The term ‘partially anonymous, partially unlinkable’ means that an a priori designated opener, and that designated opener only, can identify the authenticated entity. For example, a library may need to identify an entity that has not returned a borrowed book in order to send a late notice to the entity. Current cryptographic technologies are available to provide partially anonymous, partially unlinkable authentication. This International Standard defines a framework and requirements for partially anonymous, partially unlinkable authentication.

INTERNATIONAL STANDARD **ISO/IEC 29191:2012(E)**

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

1 Scope

This International Standard provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.

NOTE Re-identification is also called opening.