

“网络身份证”来了

可替代身份证买车票办入住等

什么是可信身份认证体系

日前,由公安部第一研究所可信身份认证平台(CTID)认证的“居民身份证网上功能凭证”亮相支付宝,在衢州、杭州和福州启动试点应用。用户只需按照提示完成“刷脸”等相关身份认证,就拥有了属于自己的“网证”。使用时打开“网证”二维码扫一扫,就能完成公积金社保查询、酒店入住登记和购买车票这些过去需要身份证才能办理的业务。这是继去年底广州签发首张“微信身份证”之后,网络可信身份认证体系的又一应用落地。

随着网络可信身份认证体系建设加速,“网证”安全日益受到关注。什么是可信身份认证体系?如何保证识别技术的准确性和安全性?怎样在认证过程中保护个人隐私和数据?记者进行了采访。

在网络中确保“你是你,而不是别人”,是通向虚拟社会的第一道“关卡”。现代社会中,身份认证的形式随着社会发展而不断演进。古代的人们出门远行,通常要去官府开具路引;几十年前,人们要去单位开介绍信;现在人们出差或旅游时,则要带着身份证。“一方面要对自然人的属性进行描述,另一方面需要一种权威的、对自然人的认证。尤其当你走出熟悉的圈子跟陌生人交往时,身份认证是一个重要的环节。”亚信安全副总裁陆光明说。

在互联网虚拟社会中,陌生人间的交往会更多,可信身份认证也就更为基础和重要,成为用户通向虚拟社会的第一道“关卡”。“网络可信身份,就是在网络接入、访问、操作、发布等各个环节,确保‘你是你,而不是别人’,确保身份可信,通过一系列安全

保障的措施,把个体纳入可信身份的体系当中。”中国网络安全审查技术与认证中心副主任王连印说。

王连印认为,随着信息化的高速发展,线上线下不断融合,越来越多现实中的行为和场景折射到网络世界中,给网络安全带来了新的挑战。“信息化发展到哪里,网络安全的问题就出现在哪里,可信身份认证体系的建设是网络安全保障的重要手段。”

我国第二代身份证的技术体系设计定位为“线下”防伪,只适用于“人证合一”的身份识别,尽管用户在网络上自证身份时,需要提供全部的身份证信息,但不能从根本上起到可信身份识别和防止冒用的作用,反而会带来泄露个人隐私信息的隐患。“网络空间的有序发展离不开可信的身份体系,它应该成为虚拟社会的通用基础设

施。”王连印说。

近年来,可信身份认证体系建设取得了显著进展。2017年6月实施的《中华人民共和国网络安全法》规定,国家实施网络可信身份战略,支持研究开发安全、方便的电子身份认证技术,推动不同电子身份认证之间的互认。《中华人民共和国电子签名法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》等法规以及相关标准的出台,使可信身份认证体系的法制环境、技术标准初步形成。

网络可信身份基础资源建设也在不断推进。公安部第一研究所和公安部第三研究所分别提出居民身份证网上副本和电子身份标识EID作为网络身份凭证。原国家工商总局则通过建设电子营业执照识别系统,解决了企业法人网络身份识别问题。

会更容易被“黑客”攻击吗

当前,国内身份认证技术产品日趋丰富,支撑了可信身份认证体系的安全发展。

当可信身份认证体系成为一种通用基础设施时,是否意味着它更容易成为“黑客”的攻击目标?

今年美国脸书公司就因“8700万用户数据外泄”事件被推到舆论的风口浪尖,让全球再次绷紧数据安全的神经。我国针对网络用户身份信息的犯罪呈逐年攀升的态势。2017年发布的《电子商务生态安全白皮书》显示,我国数十亿对账号密码关系被地下“黑色产业链”掌握,不法分子盗取、售卖用户信息获利超百亿元。陆光明认

为,身份信息本身具有巨大的商业价值,在利益驱动下,会有一些人尝试盗取身份信息,从事非法交易。“可信身份认证体系建设是网络安全保障的重要手段之一,也是网络安全的重要组成部分。”王连印说。

当前,国内身份认证技术产品日趋丰富,支撑了可信身份认证体系的安全发展。非对称加密算法、散列算法为主的基础密码技术正逐步替代国外算法,基于数字证书的身份认证技术也日益成熟,但安全性的短板仍然存在。

“网络应用系统由于使用各自的认证体系,账号无法互信互认,身份认证服务互不相通,已成为突出的问

题。”陆光明举例说,多数应用系统都独立管理用户信息,用户使用不同系统必须重复登录,设置不同的密码非常麻烦,而使用同样的密码则很容易遭受网络攻击,带来个人数据信息泄露的风险。

“如果网络服务提供商不注重用户隐私和体验,不对‘黑客’入侵、信息盗取和非法信息交易进行有效防控,就会导致用户对网络实名制丧失信心,造成企业信誉度下降,阻碍互联网发展。”陆光明表示,从这个角度看,加强顶层设计,推动数据共享,打破数据孤岛,对可信身份认证体系建设来说,是当务之急。

如何打造可信身份认证体系

要注重保护用户隐私,搭建具有政府公信力的统一身份认证平台。

“可信身份认证体系有着广阔的应用前景。”在陆光明看来,未来单维度、解决特定场景的身份认证技术将向多维度、综合性、可交叉的技术发展,安全、便捷且成本可控将成为市场应用的趋势。而实现可信身份的互联互通,需要将可信身份认证服务平台作为国家的关键信息基础设施来建设。

在实施层面,专家表示,打造可信身份认证体系,一是要保障用户身份的真实性。二是要注重保护用户身份的隐私,避免采集不必要的信息。三是

要调动各方的参与,网络可信身份认证体系不是一个分散的概念,需要政府、各行业企业、网络服务提供商以及网民都参与进来。四是搭建具有政府公信力的统一身份认证平台,使之成为网络空间具有社会公信力的身份认证的入口,发挥平台入口的价值,为社会公众提供权威的身份认证实名校验、隐私保护和信用评级等服务。

“比如,在‘互联网+政务服务’上,有了‘国家统一身份认证系统’,就能通过可信的前端认证技术保障和权威的后端身份核实机制,以及全国范围的互认通道,实现自然人和法人‘一地

注册、各地互认’和‘一次认证、全网通办’。”陆光明说。

王连印认为,在可信身份认证体系建设过程中,这一体系的建设者、运营者必须承担主体防护责任,坚持“谁建设谁负责,谁运营谁负责”。在监管层面,管理者对于重要信息系统要通过测评认证、安全审查等手段,对企业进行监督管理。“此外,可信身份认证体系作为面向应用的防护系统,不可‘为建设而建设’,一定要与实际应用相结合,在智慧社会、数字中国的建设过程中发挥应用价值。”王连印说。

(据人民网)