

德国 eID 机制对我国网络身份管理的启示

杨明慧^{1,2}, 刘孟占³, 邹翔^{1,2}, 汪志鹏^{1,2}, 饶洁³

(1. 公安部第三研究所, 上海 201204;

2. 信息网络公安部重点实验室, 上海 201204;

3. 同济大学电子与信息工程学院, 上海 201804)

摘要:网络身份管理已经成为电子商务、电子政务、社交网络等各类网络在线应用的基础。公民网络电子身份标识 eID 是网络上远程证明个人真实身份的权威性电子文件, 是一种实现网络身份管理的有效手段。如何在进行有效的身份认证的同时又能兼顾保护用户隐私是当前网络身份管理中亟需解决的问题。首先概述了当前网络身份认证中存在的问题, 然后针对德国 eID 机制在隐私保护、数据安全方面采取的措施进行了研究分析, 最后给出了德国 eID 机制对我国网络身份管理的借鉴意义。

关键词:电子身份标识; 网络身份管理; 身份认证; 隐私保护; 数据安全

中图分类号: TP309.2

文献标识码: A

文章编号: 1673-629X(2014)07-0157-05

doi: 10.3969/j.issn.1673-629X.2014.07.039

Reference of Germany eID Mechanism for China Network Identity Management

YANG Ming-hui^{1,2}, LIU Meng-zhan³, ZOU Xiang^{1,2}, WANG Zhi-peng^{1,2}, RAO Jie³

(1. Third Research Institute of Ministry of Public Security, Shanghai 201204, China;

2. Key Lab of Information Network Security of Ministry of Public Security, Shanghai 201204, China;

3. College of Electronics & Information Engineering, Tongji University, Shanghai 201804, China)

Abstract: Network identity management has become the base of on-line applications such as e-business, e-government and social network. Civil network electronic identity (eID) is authoritative electronic file to determine individual identity, which is an effective approach to implement the network identity management. However, it is a problem to protect the client's private data when carrying out the identity management in the network. In this paper, some problems of traditional identity authentication methods are described first. Then a deep analysis of Germany eID mechanism is made, especially for privacy protection and data security. The results show that Germany eID mechanism has important reference for China network identity management.

Key words: eID; network identity management; identity authentication; privacy protection; data security

0 引言

在信息社会日渐成熟的今天, 电子商务、电子政务日益成为人们日常生活中必不可少的部分。但是, 网络虚拟性、身份匿名化却制约了这些应用的发展。身份认证是验证用户身份的真实性、防止身份伪造的重要手段。网络身份认证是网络安全体系的基础, 无论是数据加密、访问控制, 还是其他网络安全技术, 都必须基于有效的身份认证^[1]。

eID (electronic Identity) 全称为公民网络电子身份标识, 是网络上远程证明个人真实身份的权威性电子文件^[2]。eID 卡可以简化在线身份认证过程并提高安全性。目前, 欧盟很多国家已经颁发了 eID 卡来替代传统的身份证, 使 eID 卡既具备了身份证的功能, 同时又具备了可靠、远程的身份识别功能。已经发行 eID 卡的国家有比利时、爱沙尼亚、意大利、德国、奥地利等, 其中比利时、奥地利、爱沙尼亚已经做到了全民

收稿日期: 2013-08-12

修回日期: 2013-11-18

网络出版时间: 2014-02-24

基金项目: 国家“863”高技术发展计划项目 (2012AA01A403, 2012AA01A404); 国家发改委下一代互联网信息安全专项试点 (发改高技 2012 [1609 号])

作者简介: 杨明慧 (1981-), 女, 博士, 助理研究员, 研究方向为网络身份管理、授权管理、信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20140224.0902.025.html>

覆盖。我国在 eID 方面的研究也取得了相应进展^[3-4]。网络身份管理试点工作得到了国家相关部委及省市的大力支持。科技部设立了公安部第三研究所负责的 eID 方面“十二五”863 重大专项和科技支撑计划项目,发改委设立了公安部第三研究所负责的 eID 方面信息安全专项和示范工程项目。相关标准化委员会决定由公安部第三研究所负责 3 项 eID 国家标准及行业标准的制定。目前已突破了多项关键技术,实现了相关产品的国产化和自主知识产权,并试点发行具有网上远程身份识别功能的 eID 卡。

在网络身份应用中,用户隐私保护是一个重要问题。现有网络身份认证技术的不足以及不科学的网络身份管理制度是导致用户隐私泄露的主要原因。2011 年末,国内知名技术开发社区 CSDN 的安全系统遭到黑客攻击,600 万用户的用户名、密码及邮箱遭到泄露。随后,天涯社区等网站相继被爆出用户数据遭泄密,互联网行业一片人心惶惶。目前网民日常使用的许多网络服务都存在泄露隐私的风险,让社会各界对网络安全和个人隐私的担忧日益加深。

在 eID 的实施和相关隐私保护方面,德国走在了世界的前列^[5]。隐私、数据安全和公民自主控制个人信息访问是其 eID 卡的主要设计目标。德国的隐私保护技术和策略与欧盟其他国家的 eID 解决方案不同,其数据最小化原则以及用户和服务提供商之间的双向认证策略为 eID 的隐私保护提供了新的方向。因此学习和借鉴德国的 eID 解决方案及相关的隐私保护策略对我国推广 eID 卡和实施网络身份管理具有重要的意义。

1 常用网络身份认证方式

随着互联网的不断发展,各类在线应用对网络身份认证的要求不断提高。节点的身份认证成为网络安全的一个重要方面^[6]。目前,网络身份认证方式主要有以下几种。

用户名/密码组合。这是最简单的网络身份认证方式。用户在线应用注册时,设定私有的密码。这种认证方式很容易遭到各种攻击,是一种不安全的身份认证方式。

动态口令。这是根据特定算法生成随机口令,每个口令只能使用一次的技术。用户进行认证时,除输入账号和静态密码之外,还必须输入动态口令,只有通过系统验证,才可以正常登录或者交易。

智能卡。智能卡由专门的厂商生产,是不可复制的硬件,由合法用户随身携带,登录时必须将智能卡插入专用的读卡器读取其中的信息,以验证用户的身份。

eID 卡。eID 卡是一种结合了“你拥有什么”和

“你知道什么”的认证手段,用户进行身份认证时将 eID 卡插入专用的读卡器读取其中的信息,输入正确的个人身份识别码(PIN)即可完成身份认证。eID 卡采用多种安全机制保护用户信息在读取、传输、存储过程中的安全性,保证用户身份信息的真实性。

2 德国 eID 的主要功能

德国于 2010 年 11 月正式发行了新的 eID 卡。与其他国家不同,德国在设计整个 eID 时就充分考虑了安全因素。例如:所有数据传输必须加密;数据的传输必须经由持卡人同意;持卡人必须知晓他们的数据传输对象;只有必要的数据才会被传输等等。正是有如此严格的安全要求,德国 eID 卡在公民个人隐私方面才能够有足够的保障。本章首先阐述德国 eID 卡的主要功能。

如图 1 所示,德国 eID 卡具有电子身份认证、电子签名和电子护照三个主要功能。

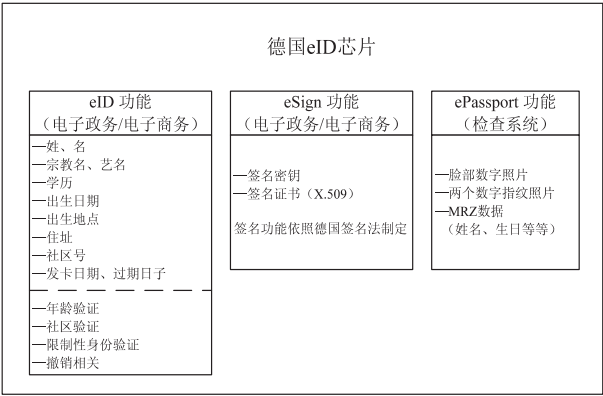


图 1 德国 eID 主要功能

(1) 电子身份认证(eID 功能)。

电子身份认证功能允许用户在电子可控的环境中证实自己的身份,常用于电子商务、电子政务,例如在线注册、网站的匿名访问、终端设施的使用等。其数据包括姓名、生日、住址等个人信息以及 eID 卡的颁发日期等卡相关信息。当持卡人需要向某种应用证实自己的身份或证明自己符合若干条件时,他使用 eID 卡并输入个人身份识别号码(PIN)以允许服务供应商访问指定的数据。

(2) 电子签名(eSign 功能)。

除了安全的电子身份认证功能外,依据欧盟电子签名指令和德国数字签名法,eID 卡中还制定了电子签名功能,来签名电子档案,例如授权书、租赁协议以及具有法律约束力的意见书等。该功能作为可选项,用户要使用则必须从经认证的服务提供商那里购买签名证书。此时,eID 功能可以向证书权威(CA)证实持卡人的身份。生成的签名密钥存储在 eID 卡中,公钥被发送到 CA,最后在线下载证书存储到 eID 卡中。

(3) 电子护照(ePassport 功能)。

德国 eID 卡的电子护照功能根据国际民航组织(ICAO)相关标准制定,等同于欧洲电子护照。该功能使用独立的数据域,与身份认证、电子签名是物理和逻辑分离的。其数据包括个人数字照片、两个数字指纹和一些个人信息。这些数据的访问是受限的。只有授权机构,例如警察、边境控制机关等才能访问电子护照。

以上三个功能中,应用最多、与公民日常生活关系最为密切的是 eID 功能。由于需要存储、传输、处理大量的个人信息,其个人隐私保护问题也最为重要^[7]。对此,德国采取了多种安全机制保护公民的隐私数据安全。

3 德国 eID 的安全机制

德国在设计 eID 时,充分考虑了个人隐私、数据安全和个人信息的自主访问控制。双向认证策略和数据最小化原则是其保障数据安全的重要手段及与欧盟其他国家不同之处。本章将从安全认证协议及数据最小化原则两方面详细介绍德国 eID 的安全机制。

3.1 eID 中的安全协议

德国 eID 卡的安全协议和 PKI 基础设施共同确保个人数据的安全以及 eID 卡的真实性,防止信息伪造^[8]。德国信息安全联邦机构(BSI)带领和参与开发了以下协议和方法并建立了相应的公钥基础设施,如表 1 所示。

表 1 安全协议和方法

简写	全称	作用
PACE	Password Authenticated Connection Establishment	访问控制,防止远距离读取芯片
PA	Passive Authentication	验证芯片中数据的真实性和完整性
	Extended Access Control	扩展访问控制,包括两个子协议
EAC	CA:Chip Authentication	建立安全连接,检测“克隆”芯片
	TA:Terminal Authentication	当终端设备读取芯片时认证终端设备
RI	Restricted Identification	创建芯片与网络服务对应的假名
	Public Key Infrastructure	公钥基础设施,包含证书层次结构
PKI	CSCA:Country Signing Certificate Authority	该层次的数字证书用于电子签名
	CVCA:Country Verifying Certificate Authority	该层次的数字证书用于控制读取权限

eID 卡需要两个公钥基础设施(PKI):一个是国家签名证书颁发机构(CSCA),用于验证电子身份档案的真实性;另一个是国家认证证书颁发机构(CVCA),用

于保护电子身份档案中的指纹信息。

CSCA 由 BSI 运作。该机构定期生成用于签名的根证书(CSCA 证书)。CSCA 证书是 CSCA 公钥基础设施的基础。为验证不同国家电子身份档案的真实性和完整性,各个国家必须以安全的方式交换各自的根证书,例如外交途径或者 ICAO 公钥簿。

CVCA 也由 BSI 运作。该机构定期生成用于认证的根证书(CVCA 证书)。证书的私钥用于对档案校验器的档案校验证书进行签名。其他国家若要使用德国 eID 卡的相关功能,其权威机构也需要获得相应的授权证书。

除了上述两个公钥基础设施外,BSI 还开发了用于不同认证目的的安全协议,包括密码认证连接(PACE)、扩展访问控制(EAC)和反向认证(PA)等。

PACE 协议主要用来保证 eID 卡中的非接触式芯片不被非法读取,并确保芯片与终端设备交换数据是以加密的形式完成的^[9]。PACE 密码取决于所使用的终端设备(读卡设备)的授权证书,通常是六位的 PIN 码,只有持卡人自己知道。PACE 的优点是密码长度不会影响加密的安全等级。也就是说,即使使用相对较短的 PIN 码,eID 卡中的数据在传输过程中也可以得到高强度的保护。

PA 协议旨在验证 eID 卡的芯片中数据的真实性和完整性。制造 eID 卡时,制造商用自己的签名证书对芯片中的数据进行签名,而该签名证书正是用上文提到的 CSCA 证书进行签名的。根据 PA 协议,当终端设备读取 eID 卡中的身份档案时,需要验证芯片中所存数据的签名,并追溯到 CSCA 证书。这样终端设备可以确定身份档案中的数据是官方授权的 ID 制造商写入的,并且是未经修改的。

EAC 协议包括芯片认证(CA)协议和终端认证(TA)协议。这两个协议与 PACE 协议及 PA 协议一起使用。

CA 协议的目的是确保芯片的真实性,并且在芯片和读卡器之间或者芯片与服务提供商之间建立安全连接。芯片认证基于 Diffie-Hellman 密钥交换技术。密钥交换过程中,读卡器或终端设备使用临时密钥对,而芯片使用静态密钥对。同时,在芯片和服务提供商之间建立高强度加密的端到端的通道。

eID 卡中的所有数据都是保密的,必须防止未经授权的人读取这些数据。TA 协议就是为此开发的。读卡器只有成功执行该协议后才能读取敏感数据。电子身份文档中的芯片的设计原则是:读卡设备只有证明其具有特定的读取权限后,才能读取特定的数据。存储在芯片中的 CVCA 证书正是用来验证相应的读取权限。

终端认证过程中,终端将其读权限以终端证书的形式传送给芯片。同时还会传递 CVCA 证书和证书层次结构中位于这两个证书之间的所有证书。这样,芯片就可以验证终端证书的真实性和完整性。从 CVCA 证书开始,证书层次结构中每一个后续的证书都要用前一个证书的私钥签名。而制造商制造芯片时会将该证书存储在芯片中,所以芯片可以确信自己存储的证书是可信的。

一旦验证了终端证书的真实性和完整性,芯片必

须验证该证书确实属于该终端设备。为此,芯片会向终端设备发送一个随机数,终端设备用自己的私钥对该随机数签名并将签名后的随机数传回给芯片。芯片可以利用终端证书中设备的公钥验证该随机数签名的合法性并判定终端设备是否具有与证书匹配的私钥。

德国 eID 的安全机制与其他国家的不同之处在于其支持双向认证机制^[8],即用户和服务提供商之间相互认证对方的真实性,这是通过上述安全机制实现的。图 2 所示是其网络应用认证的大致流程。

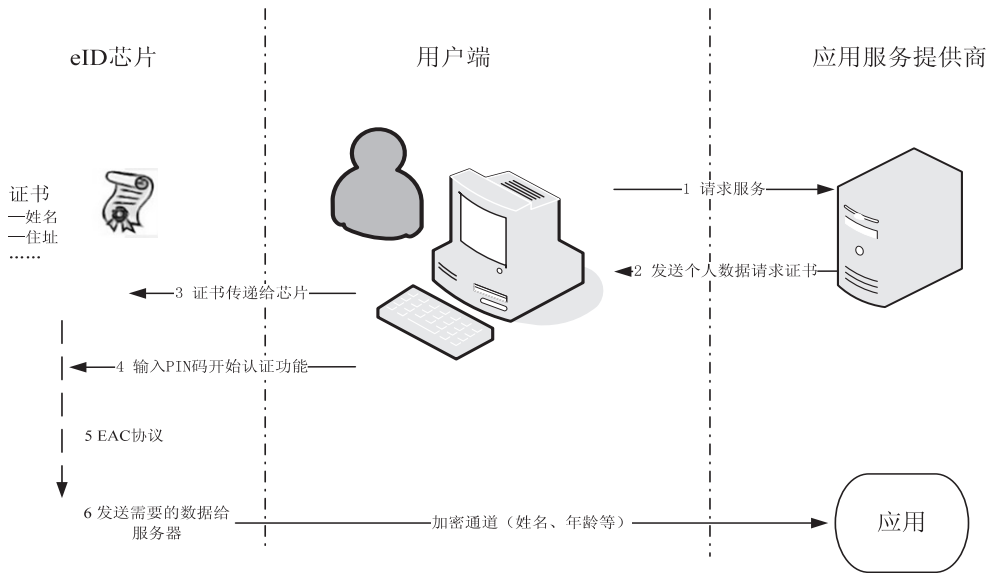


图 2 德国 eID 认证流程

- 第一步,用户向应用服务器发送服务请求;
- 第二步,服务器返回给用户所需个人数据的请求证书;
- 第三步,该证书信息传递给读卡设备;
- 第四步,用户插入 eID 卡,输入 PIN 码开始认证功能;
- 第五步,执行 EAC 协议,完成用户与服务器的双向认证,并建立高强度的加密通道;
- 第六步,发送需要的数据给服务器,完成最终认证。

在德国 eID 机制中,服务提供商读取 eID 卡中的个人数据时,必须出示其读取权限证书,认证通过后,还必须向用户展示其要读取 eID 卡中的哪些个人数据,最终由用户决定是否允许其读取这些个人数据。这样可以有效避免钓鱼网站骗取个人隐私数据,防止泄漏个人隐私。

3.2 eID 中的数据最小化原则

数据最小化原则^[10]是指只收集或者保存必需的数据,而不访问额外的任何信息。德国 eID 卡支持三种数据最小化功能。

(1)年龄验证。某些服务需要验证用户的年龄。数据最小化原则要求:年龄认证功能不会传输精确的

出生日期。服务提供商只能确定用户年龄是否达到要求的年龄,例如 16 岁或者 18 岁。服务提供商向芯片发送一个参考数据,并与出生日期比较,然后返回“yes”或者“no”。

(2)居住地验证。区域服务提供商需要检测用户是否在特定的区域或城市。居住地验证功能不会传输完整的住址,而仅仅比较 eID 卡持卡人的区域标识符和服务提供商发送的参考区域标识符,并返回“yes”或者“no”。

(3)限制性身份认证(假名功能)。网上论坛或网络聊天通常都需要填写个人信息。如果使用 eID 卡,持卡人不必泄漏任何个人信息就可以使用该类服务。服务提供商可以使用特定的标识符(假名)识别某个用户是否是 eID 卡的所有者。该特定的标识符是由 eID 卡的密钥和服务提供商的标识符进行某种计算得出的,服务提供商的标识符是其授权证书的一部分。对于每一个服务提供商,持卡人的假名都是不同的。计算过程不需要用户输入任何数据,但是服务提供商读取用户假名需要用户输入 PIN 码。

可见,数据最小化原则使得用户能够在提供尽可能少的个人信息的情况下,正常使用服务提供商提供的服务,有效地保护用户的个人隐私。

4 对我国网络身份管理的启示

在我国,人们日常使用的许多网络服务都存在安全隐患。在线服务要求个人信息作为身份证明,服务提供商访问个人信息不受控制^[11]。eID 作为公民网络电子身份标识,包含了更多的个人隐私信息,一旦投入使用,其个人隐私保护问题将更为突出。我国网络身份管理制度的设计理念与德国 eID 卡的设计理念一致,都把用户隐私作为首要的考虑因素。Christian J. Dietrich 等人^[12]已经理论上证实德国 eID 卡是安全可靠的。其 eID 解决方案及相关的隐私保护策略对我国推广 eID 卡和实施网络身份管理具有重要的意义,可以借鉴如下:

首先,需要明确双向认证的身份认证机制。通常,身份认证过程中,服务提供商需要验证用户身份的真实性。用户需要填写大量的个人信息来注册或者使用某项服务。一方面,这样容易泄露用户自身的隐私信息,另一方面,用户无法确信服务提供商的身份是否真实可靠。德国的双向认证机制不但在终端保障了 eID 数据的安全,验证了用户身份的真实性,而且由于需要服务提供商提供相应的证书,也认证了服务器身份的真实性,避免了一些不良网站的危险,并且还在用户与服务器之间建立了高强度的加密通道,保障了数据传输的机密性。

其次,需要遵循数据最小化原则。数据最小化原则中的限制性身份认证中,服务提供商只能得到用户身份真实性与否的信息,不能得到用户的详细的身份信息(例如,姓名,出生日期等),这样避免了服务提供商滥用用户身份信息。即使服务提供商的系统被攻破,也不会有隐私泄露的威胁。此外,服务提供商读取特定身份信息时,eID 卡会验证服务提供商的读取权限,并展示其要读取的细节数据,由用户确定是否允许读取。该原则避免了不必要的隐私信息传输,最大限度地隐藏了用户的隐私信息。

最后,需要完善个人隐私保护规定。德国在网络身份管理上有很完善的法律法规,其 eID 的设计有相应的规范作为依据。而我国只颁布了电子签名法^[13]等法律法规,缺乏完善的数据保护法,也未形成体系化的隐私数据保护制度。

因此,需要协同政府、行业和监管部门,进一步明确网络身份管理中隐私保护原则、保护范围、数据控制者义务等内容。例如,禁止服务提供商长期保留用户的身份信息;建立统一的身份认证机构对使用用户身份信息的服务提供商进行监督管理,等等。

5 结束语

网络身份应用管理中,用户个人隐私保护是一个重要问题。在 eID 的实施和相关隐私保护方面,德国走在了世界的前列。文中大致介绍了德国 eID 的主要功能,深入剖析了其安全机制,总结了其对我国网络身份管理,尤其是用户隐私保护方面的借鉴意义。

我国网络身份管理还处于初步发展、试点应用的阶段。然而,安全机制,尤其是 eID 相关的隐私保护机制必须在设计时就充分考虑。需要借鉴各国成功或失败的经验,从技术上、体制上、管理上维护公民在网络空间的合法权益,保护公民的个人隐私,构建安全可信的网络空间。

参考文献:

- [1] 罗 斌,裘正定.网络身份认证新技术[J].计算机安全,2005(10):29-31.
- [2] 公安部第三研究所.认识 eID[J/OL].2013. <http://www.eid.cn/introduce1.html>.
- [3] 顾 青,梁佐泉,汪 治,等.网络身份识别系统在电子商务中的研究与应用[J].计算机技术与发展,2011,21(11):247-249.
- [4] 孙印杰,陈智芳,王 敏,等.基于指纹和数字水印的网络身份认证系统研究[J].计算机技术与发展,2008,18(4):147-150.
- [5] 上官晓丽.国际身份管理和隐私保护标准研究[J].信息技术与标准化,2012(1):27-32.
- [6] 任 方,马建峰,钟焰涛.PKI 技术在空间信息网中的应用[J].计算机科学,2011,38(1):51-53.
- [7] Poller A, Waldmann U, Vowe S, et al. Electronic identity cards for user authentication – promise and practice[J]. IEEE Security & Privacy, 2012, 10(1):46-54.
- [8] Noack T, Kubicek H. The introduction of online authentication as part of the new electronic national identity card in Germany [J]. Identity in the Information Society, 2010, 3(1):87-110.
- [9] Jens Bender J, Kügler D, Margraf M, et al. Sicherheitsmechanismen für kontaktlose chips im deutschen elektronischen Personalausweis[R]. [s. l.]:[s. n.], 2008.
- [10] Fumy W, Paeschke M. Handbook of eID security[M]. [s. l.]:Wiley-VCH, 2011.
- [11] 第 31 次中国互联网络发展状况统计报告[R/OL]. 2013. <http://www.cnnic.cn/hlwfyj/hlwzxbg/hlwtybg/201301/P020130122600399530412.pdf>.
- [12] Dietrich C J, Rossow C, Pohlmann N. eID online authentication network threat model, attacks and implications [C]//Proc of 19. DFN workshop. [s. l.]:[s. n.], 2012.
- [13] 刘左军,黄建初.中华人民共和国电子签名法[M].北京:中国民主法制出版社,2004.

作者：[杨明慧](#)，[刘孟占](#)，[邹翔](#)，[汪志鹏](#)，[饶洁](#)，[YANG Ming-hui](#)，[LIU Meng-zhan](#)，[ZOU Xiang](#)，[WANG Zhi-peng](#)，[RAO Jie](#)

作者单位：[杨明慧, 邹翔, 汪志鹏, YANG Ming-hui, ZOU Xiang, WANG Zhi-peng \(公安部第三研究所, 上海 201204; 信息网络公安部重点实验室, 上海 201204\)](#)，[刘孟占, 饶洁, LIU Meng-zhan, RAO Jie \(同济大学 电子与信息工程学院, 上海, 201804\)](#)

刊名：[计算机技术与发展](#)

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014(7)

参考文献(13条)

1. [罗斌;裘正定](#) [网络身份认证新技术](#) 2005(10)
2. [公安部第三研究所](#) [认识eID](#) 2013
3. [顾青;梁佐泉;汪治](#) [网络身份识别系统在电子商务中的研究与应用](#) 2011(11)
4. [孙印杰;陈智芳;王敏](#) [基于指纹和数字水印的网络身份认证系统研究](#) 2008(04)
5. [上官晓丽](#) [国际身份管理和隐私保护标准研究](#) 2012(01)
6. [任方;马建峰;钟焰涛](#) [PKI技术在空间信息网中的应用](#) 2011(01)
7. [Poller A;Waldmann U;Vowe S](#) [Electronic identity cards for user authentication-promise and practice](#) 2012(01)
8. [Noack T;Kubicek H](#) [The introduction of online authentication as part of the new electronic national identity card in Germany](#) 2010(01)
9. [Jens Bender J;Kügler D;Margraf M](#) [Sicherheitsmechanismen für kontaktlose chips im deutschen elektronischen personalausweis](#) 2008
10. [Fumy W;Paeschke M](#) [Handbook of eID security](#) 2011
11. [第31次中国互联网络发展状况统计报告](#) 2013
12. [Dietrich C J;Rossow C;Pohlmann N](#) [eID online authentication network threat model, attacks and implications](#) 2012
13. [刘左军;黄建初](#) [中华人民共和国电子签名法](#) 2004

引用本文格式：[杨明慧](#).[刘孟占](#).[邹翔](#).[汪志鹏](#).[饶洁](#).[YANG Ming-hui](#).[LIU Meng-zhan](#).[ZOU Xiang](#).[WANG Zhi-peng](#).[RAO Jie](#) [德国eID机制对我国网络身份管理的启示](#)[期刊论文]-[计算机技术与发展](#) 2014(7)