**CPK可证网络**

南湘浩

摘要：本文回顾了40多年信息安全发展所走过的历史，以新的视野分析了经验与教训，从理论上探讨了物联网和事联网安全的本质、安全原则、安全策略、安全方法等，最终形成了以物联网实体鉴别和事联网事件鉴别为主的网际安全的概念。这对电子商务，未来网的建设，网络管理，尤其作为网络战的应对措施都具有重要意义。

关键字：自主可控，事联网，实体鉴别，事件鉴别 虚拟链接

我们经历了线路通信点对点的通信保密、局域网的数据鉴别、因特网的用户鉴别，物联网的实体鉴别，正经历事联网的事件鉴别。在发展过程中也产生过不同主张和不同概念。本文试图论述自主可控安全策略与事联网概念以及最后形成的总体解决方案。

**1 与时俱进**

信息安全是由Information security翻译而来，但我国至今没有给出准确的定义，但一般遵从克林顿的PDD63中给出的定义，即脆弱性分析、堵漏洞、打补丁。于是，防火墙、入侵检测等技术潮水般引进来了。当然，脆弱性分析是信息安全的内容之一，是否主要内容，答案是否定的。结论已在布什政府的PITAC的报告《网际安全--优先项目危机》中已给出：不是脆弱性分析，而是鉴别技术。从美军网络战的实验情况看，只抓住了两个核心问题，即：非法入侵，权利接管。美军还宣称，对方数据库的每一字节都能控制。那么如何防止非法入侵、防止权力被接管，这就要靠鉴别技术。

以公开的技术做到保密是最好的保密技术，而互联网又是人类命运共同体，因此，任何先进技术都是人类共同的财富。过去由于某种原因，国内情况谈论的不多，现在了解国内真实情况的人几乎没有剩几个人。知己知彼，才能百战不殆。当真实了解了自己，才能避免出现“骑驴找驴”，“端着金饭碗要饭”的可笑局面。

四十多年来，我们经历了几个发展阶段，基本上都是与时俱进的。在不断缩短与发达国家的差距的同时，有些关键技术甚至超越国际先进水平。

1970年代，通信速率的急速提高，便产生了加密作业电子化的需求。我们研制了电子密码机M06，进入了点对点(point to point)的通信保密年代，将与发达国家的差距从40年拉到10年。通信保密的主体是数据，安全课题主要是数据保密。

1980年代，我国引进了一种大型计算机网络（封闭的专用网），局域网打破了各终端的界限，产生了共享资源，进入了共享资源中以数据鉴别为主的端对端（end to end）的发展阶段。数据鉴别采用分级管理的强制控制解决共享资源中的数据。以DoD橘皮书为代表[1]。美国只提出了文本，但由于互联网的出现则停止了局域网的研究，而我国国防网是用基于标识的TLK（对称密钥和非对称密钥结合的两层密钥）技术实现了“918系统”，解决了全军网规模化密钥管理问题，并实现了多级管理的数据鉴别，使我国成为率先使用基于标识的密钥体制的国家和率先进入网际安全阶段的国家。

1990年代，互联网开始普及，打破了局域网的界限，最终形成了以用户鉴别（user authentication）为主的用户对用户（user to user）的互联网的新时代。我国提出的基于标识的多层公钥LPK[1][2]，在SJY01中得到应用，解决了超大规模用户鉴别问题，其性能大大优越于基于CA的PKI。克林顿政府虽然历史性地提出互联网的安全靠全体网民自行保护的自主控制的（assurance）策略，但是因特网安全却只关注了堵漏洞、打补丁的脆弱性分析，将互联网用户安全引入了系统安全。这是在形象思维模式下得出的结论，没有分析出实质行问题，以总统令PDD63为代表[2]。

2000年代，物联网的出现，将信息网络（互联网、移动网）包括在非信息网络（物联网），并将网络与社会生活结合在一起，进入了物对物（thing to thing），实体对实体（entity to entity）的物联网时代。美国人称“cyber security”（网际安全），以美国总统信息技术顾问委员会（PITAC）报告《网际安全》为代表[3]。报告提出了“互相怀疑”的安全原则，以解决数十亿规模的“鉴别技术”为主要目标，构建可信世界作为主要任务。这是在抽象思维模式下分析出来的结论，抓住了实质性问题，但至今没有找到解决办法。而在我国已用标识概念将互联网、移动网、物联网等统一到一个网际空间，提出了基于标识的组合公钥CPK[4][5]，解决了作为“网际安全的银弹”的标识鉴别（identity authentication）,并应用于实体鉴别中。

2010年代，随着电子商务和网络战的发展，网络犯罪和网络恐怖活动频频发生，于是便产生了在网际空间中对“事件”鉴别的迫切需求，如通信中非法接入事件，在交易中假冒顶替作案的事件等，于是悄悄引起了静态的物联网（IoT）的“实体鉴别”，向动态实体的“事件鉴别”的发展。实体的互动构成“事”或“事件”，任何事件均以过程形式存在，而过程产生虚拟链接，而虚拟链接构成事联网。我们创建了对实体、事件都能证明真实性的“真值逻辑”[6][7]。于是我们率先进入了以事件鉴别（event authentication）为核心的事联网（Internet-of-Event）时代。

纵观与信息技术（IT）同步发展的鉴别技术的历史可看出，其发展轨迹是很清楚的，即从数据鉴别、用户鉴别、实体鉴别最后发展到了事件鉴别。由于万物是由各种各样的实体构成的，而实体的运动必然形成事件。因此只要抓住实体鉴别和事件鉴别这一根本问题，其他“安全”问题就可以迎刃而解。而实体鉴别和事件鉴别的基础是标识鉴别，因此标识鉴别是网际安全的“纲”。

**2 三种差异**

网际安全的研究对象经历了从封闭的集团化局域网到开放的个人化公众网的重大变化。美国总统信息技术顾问委员会（PITAC）研究人员和我国民间QNS工作室研究人员共同认为，公众网的安全要从过去被动防御型安全要转变为主动管理型安全。但是在美国的研究和中国的研究比较起来，差异还是有的，归结起来有以下三点：

第一个差异是在核心技术的认定上，美国PITAC第一次提出网际安全的原则是“互相怀疑”，核心技术是“鉴别技术”。这是划时代的提法，于是在美国兴起了各种鉴别技术的研究，如指纹识别、面部识别技术等。但后来发现，物理的、生物的鉴别技术只对当面鉴别有意义，对远程鉴别则意义不大，对远程鉴别仍束手无策。而我国民间QNS则提出了“标识鉴别”和“事前鉴别”课题，解决了非法接入和远程鉴别问题。2007年11月新华社内参刊登了“我解决世界难题的‘电子身份证’，引起国际关注”的文章，胡锦涛做了批示，但没有引起相关部门的注意，没有成为国家的意志，仍停留于民间的层次上。实际上，基于标识构建的鉴别网络具有“独立性”和“溯源性”，为构建自主可控网络体系，防止非法接入提供了基础依据。现行的因特网之所以能随意发生非法入侵，就是因为它不提供源地址证明。这对美国有利，因为译名服务器在美国，美国对我们的网络行为了如指掌，而我们对美国的网络行为却一无所知。

第二个差异是在主要任务的认定上，美国PITAC要建立的是“可信世界”，而我们QNS要建立的是“可证世界”。“可信性”是主观把握，而“可证性”是客观判断。美国虽然提出了“互相怀疑”的原则，但还没有从信任逻辑中摆脱出来。根据我们的经验，可信逻辑到可证逻辑的转变并非易事，因为它关系到鉴别理论的基础，为此我们从基于行为的信任逻辑，从基于模型的相信逻辑的束缚中解救出来，创立了基于证据的新型鉴别逻辑--真值逻辑。其实，道理是很浅显的，如一个人到商店买东西，售货员和顾客互不认识，没有信任可言，但买卖却做成了，证明交易与信任无关，却与交易内容有关，即所付的钱是真实的，拿的东西是真实的。另外，信任还有更可怕的性质，即信任的转移特性。现在有些系统是建立在信任转移链上。这种基于信任的的安全机制，实际上已变成了安全隐患，如基于信任的网络连接和口令认证变成引发非法入侵的祸根，如基于信任转移的登录（注册）机制变为引发权利被接管的祸根。美军的网络战正是利用了这两个“安全机制”的弱点进行的。

第三个差异是研究路线上。美国人走的是理论先行的路，在理论指导下开展技术开发活动。美国之所以先进，主要体现在他提出了符合时代需求，具有指导意义的很多新概念。如：Denning的自主控制和他主控制的数据库管理的安全策略概念、DoD在资源共享体制下的等级划分的信息安全概念，在互联网条件下靠全体网民共同维护安全的assurance概念；物联网和Cyber Security 概念等等，公布了一批公钥体制，如DLP、RSA、ECC等，制订了数字签名标准等，起到了引领全球的作用。尽管对标识鉴别的认识滞后于中國，但是到了2011年奥巴马政府把布什政府的“鉴别技术”改为“标识鉴别”，并把标识鉴别正式作为美国国家战略，已形成为国家的意志。PITAC把标识鉴别当作“银弹”（万能药），但可惜，至今没有找到解决办法。中國所走的路，官方和民间不同。官方走的路是“跟随”美国走，跟随策略本来没有错，也符合发展的一般规律，但由于理解错误和翻译错误，不仅没有跟对，反而起到全国性的误导作用。美国国防部曾匆忙编制了“Information Assurance Technical Framework”（IATF）一书。此书由于过分宣杨“信息孤岛”和“边界保护”的错误观念，将开放的互联网引向支离破碎的封闭网而受到美国政府的批判。在这种情况下，此书在中国仍被当作宝书全国推广。更为甚者，把“Assurance”（自主）理解成“Guarantee”（保障），调换了概念，其流毒影响了整个互联网时期。民间所走的路是先解决实际问题，再提升到理论。由于理论落后，容易陷入“盲目”。2002年，当看到1984年Shamir的IBC论文才知道原来还有基于标识的公钥体制。实际上1989年在全军国防网上用的就是基于标识的密钥体制，但当时并不知道，更不可能提高到理论的高度。十多年来，通过防量子计算攻击、鉴别逻辑、自主可控、虚拟链接等理论研究，越来越感到理论的重要性。虽然在某些实用成果超出了发达国家水平，但在重视理论研究的意识方面、国民对新概念、新理论的接受能力方面还存在相当大的差距。重视理论的发展是发达国家或创新性国家的特点。

**3 两大威胁**

根据网络战和网络犯罪的分析，在信息空间中存在两大威胁。一是非法入侵；二是权利接管。

非法入侵是网络战或网络犯罪的第一需求，而目前的防范措施很弱。目前普遍采用的是“口令认证”或指纹识别等生物特征。如果口令认证或生物特征用于当面鉴别，是一种理想防非法入侵的方法，如打开自己的计算机、手机等。但是用在远程鉴别就不合适了。实际上口令给对方内部作案提供了条件，而生物特征在网上就失去了其特性。很显然，在远程鉴别中无论是口令认证和生物特征，其防御能力都显得很弱，怪不得某外军声称：可以随时入侵对方系统，成功率为百分之百。

权利接管是网络战或网络犯罪最终达到的目的，而且是越来越发展的领域。一个恶意软件要起作用，必须取得权利。获取权利的方法很多，有的是利用系统本身的漏洞，有的是利用传统的安全机制的原理。至今把登录机制作为安全机制来使用。而登录机制不可避免产生信任链。登录一次不仅处理一件事，接着可以处理第二件事。这种信任的转移容易引起权利的转移，为敌方提供可钻空子的机会。一旦权力被接管，那么入侵者就可以随心所欲地进行它的活动。于是某外军声称，他们可以控制到对方数据库的每一字节，甚至可以入侵雷达系统，控制对方的显示屏幕，随意替换画面。

**4 自主可控**

自主可控是作为安全机制来提出来的，但有些人将自主可控与国产化、主权、话语权混淆起来。首先自主可控与国产化是毫无相干的两个问题。我们不能说国产车安全，进口车不安全，主要看采用了多少安全措施。其次自主可控与主权问题，也是属于不同范畴的问题。主权是领地概念，指所有权和管辖权，其特点是有边界。至今，主权问题只停留于政治口号，对网络空间没有给出准确的定义，对主权的存在性也没有给出证明。但有一个共识：互联网没有边界，互联网是人类命运的共同体。而主权要求就是要划定边界的，那么这种要求是历史的进步还是退步？关于话语权问题，在技术开发过程中，曾碰到过话语权问题。本来对我们来说，在解决了标识鉴别课题的基础上，在互联网的路由器上做源地址证明并不难，实际上我国已研制成功了IPv9，采用了实名地址，提供源地址证明。但是IPv9与现行的IPv4, IPv6不兼容，需要修改IP协议，这就不得不涉及到国际上的话语权。这种话语权也许是靠民主的多数表决，也许是靠资本的股权的多少来决定，因为我们在互联网的会议上不属于大多数、也不是大股东，自然就没有决定性的话语权。在这种情况下，避免这种尴尬局面的唯一的捷径，就是构建自主可控的网络。于是2012年提出了构建自主可控网络系统的建议（刊登于人民日报内参）。在商业化运作的机制中，我们与首先遵守“游戏规则”，想要得到更大的话语权，需要加大资本股或技术股，别无它法。而加大技术股的根本途径在于创新。

自主可控的另一种解释是从技术层面上的安全控制机制，称安全策略。有一种说法：“我的安全我做主”，“我的账户我来管”，通俗地刻画了自主可控的含义。直到目前，安全控制形的式只有两种：一是靠自己意愿的控制的自主控制，二是被迫执行他人规则的他主控制。后者也称强制控制。自主可控问题直接涉及到控制的依据、控制对象、控制方法。控制依据则由鉴别逻辑提供。在实体真实性证明中，一个实体分为两部分：标识和本体。标识是代表实体的名称，满足唯一性、公认性、可证性即可。本体是实体本身，以本体特征（物理的、生物的、逻辑的）来代表。标识证明和本体证明可独立进行。CPK鉴别系统采用基于证据的证明逻辑，所有证明系统均由示证系统和验证系统构成。根据“互相怀疑”的安全原则，对任何实体进行真伪鉴别，为自主可控提供判别依据。

自主可控是由主动方提供真实性证据，由被动方实施控制的方式进行的。下表4.1给出了几个例子：

表4.1 被动方自主可控模式

|  |  |  |
| --- | --- | --- |
| 事件 | 主动方 | 被动方自主可控的模式 |
| 通信事件 | 发方对发方真实性的证明  发方对收方真实性的证明  发方对数据真实性的证明 | 收方对受理与否的控制  收方对受理与否的控制  收方对采纳与否的控制 |
| 办公事件 | 创建方对创建人真实性证明  创建人对数据真实性证明 | 文件阅读方对受理与否的控制  文件阅读方对采纳与否的控制 |
| 软件事件 | 发行方对发行方真实性证明  发行方对软件名真实性证明  发行方对软件体真实性证明 | 使用方下载（加载）与否的控制  使用方下载（加载）与否的控制  使用方安装（执行）与否的控制 |
| 支付事件 | 支付方对支付方真实性证明  支付方对收款方真实性证明  支付方对金额真实性签名 | 收款方对受理与否的控制  收款方对受理与否的控制  收款方对采纳与否的控制 |

自主可控是网际安全的基本要求，也代表着安全系统发展的方向。自主可控至少具有独立性和可证性。独立性为事件提供自主处理的基础，保证不被他主处理；而可证性为用户自主可控提供控制依据。自主可控系统的建设要做到：在网络战中的“我方识别”，在情报战中的“不怕窃密”，银行系统中的“不怕泄露”。

现在自主可控的概念越来越深入人心，越来越多的系统自觉实行自主可控的安全机制，但仍有很多系统以破坏自主可控原则来提供“安全服务”，如强行要求用户输入口令、强行与某些参数绑定等。甚至有的系统（区块链）将账户共同管理的名义，侵犯账户自主可控的管理。这些做法都是在没有解决相应技术条件下的不成熟的半成品，也许能解决眼前的某些问题，但阴藏着更大的危险。

**5 虚拟链接**

世界是由实体构成的，静态的实体构成物联网。物联网的核心是证明实体真实性。实体真实性证明是通过标识鉴别和本体鉴别来实现的。而动态的实体会怎么样？任何实体之间的互动，产生一个“事件”并自动形成虚拟链接。虚拟链接是从实体标识到实体标识的链接，即I to I模式。事件是以过程形式体现的。事件的过程分为接入（受理）进程和接收（采纳）进程。受理近程总是在接受进程之前发生，为接受进程发生之前对事件的真伪做出判断提供了条件，称事前鉴别。

两个实体的互动产生虚拟链接。因此，只要有事件发生，就会产生虚拟链接，实体的单一活动，构成单一事件，单一事件形成单一虚拟链接，实体的复合活动，构成符合事件，复合事件形成复合虚拟链接。虚拟连接是从实体标识到实体标识的可证链接。每一事件的真实性证明都在实体真实性证明的基础上进行。由于标识是唯一的，因此各实体互为独立，各事件之间也互为独立，进而各事件所形成的虚拟链接之间也互为独立。这种独立性，给系统安全性证明带来极大方便，过去无法证明的，现在变得容易证明了。因为只有单一事件才能准确勾画出安全的特性，因此将复合事件逐一分解为单一事件至关重要。一个好的总体解决方案应是各事件有机而完整的证明鏈。

虚拟链接具有独立性和溯源性特征。将安全问题从形象化思维提高到虚拟化抽象思维考虑时，我们就能得到更加合理的解释和形成更加合理的解决方案。

**6 虚拟网络**

每一个事件都有独立性，因此可构成独立的虚拟网。根据事件和业务类别，可组成各种不同的、独立的虚拟网。虚拟网是用虚拟连接实现分类业务安全的网络。我们已经搭建了虚拟因特网、虚拟移动网、虚拟票据网、虚拟办公网等演示系统，取得了预期的效果。

**虚拟互联网（Inter-net）：**是在用户名到用户名之间，手机号码到手机号码形成虚拟链接的可证逻辑网络，提供源用户名或电话号码的真实性证明，供收方实施受理控制和采纳控制，在互联网发生的任何非法事件，最终均能在虚拟链接中被发现，被阻止，因此可以弥补通信网的安全缺陷。

发送方提供的发送方标识（sender）真实性的证据，收方真实性证据和数据真实性证据：

SIG*sender*(time)=(*s*1,*c*1)=sign1

SIG*sender*(receiver)=(*s*2*,c*2)=sign2

SIG*sender*(data)=(*s*3,*c*3)=sign3

接收方受理与否的控制：

VER*SENDER*(time,*s*1)=*c*1’

VER*SENDER*(receiver,*s*2)=*c*2’

接收方接收与否的控制：

VER*SENDER*(data,*s*3)=*c*3’

**虚拟标签网（Label-net）：**是发货者和取货者之间形成虚拟链接的可证逻辑网络。发货者提供发货者真实性证明和货物真实性证明供取货者验证。当一个收货者变为出售者时，出售者必须追加自己的真实性证明，于是形成真实性的证明链。货物的证明包括货物的标识和货物的特征值，其真实性证明均由数字签名提供。防伪标签的证明鏈和收据（发票）的证明链，共同起到防复制的作用，因此防伪标签可以是RFID，也可以是纸质的。

发货者（consignor）提供的证据是发货者的真实性和货物的真实性：

SIG*consignor*(time)=(*s*1,*c*1)=sign1

SIG*consignor*(chr)=(*s*2,*c*2)=sign2

收货者验证发货者的真实性（事前鉴别）：

VER*CONSIGNOR*(time,*s*1)=*c*1’

收货者验证货物的真实性（事后鉴别）：

VER*CONSIGNOR*(chr,*s*2)=*c*2’

**虚拟软件网（Soft-net）：**是在软件发行者和软件运行者之间形成虚拟链接的可证逻辑网络。在虚拟计算网中，发行者（issuer）提供发行者真实性证明，发行者对软件真实性证明，供使用者分别用于软件的下载（加载）或安装（执行）的判别，对软件可实行商标化管理。如果原有内核负责软件的运行安全，CPK内核负责软件的真实性，那么在虚拟计算网上可组成双内核的操作系统。

发行者提供的证据：

SIG*issuer*(time)=(*s*1,*c*1)=sign1

SIG*issuer*(chr)=(*s*2,*c*2)=sign2

用户下载软件或加载软件时的验证：

VER*ISSUER*(time,*s*1)=*c*1’

用户安装软件或执行软件时的验证：

VER*ISSUER*(chr,*s*2)=*c*2’

其中，chr可以是程序体的压缩码。

**虚拟支付网**（Pay-net）**：**支付事件是复合事件，主要由付款事件和结账事件以及收据事件构成。付款事件是在付款方和收款方之间形成的可证逻辑网络，结账事件是在收款方和银行之间形成的可证逻辑网络。

付款事件是在付款方和收款方之间发生。

1. 在远程付款时，付款方和收款方的可证连接（略）；
2. 付款方向收款方提交付款。付款包括账号真实性证明、金额真实性证明、资金流向真实性证明；如：

SIG*payer*(time)=(*s*1,*c*1)=sign1

SIG*payer*(amount)=(*s*2,*c*2)=sign2

SIG*payer*(payee)=(*s*3,*c*3)=sign3

结账事件是在收款方和银行之间发生。

1. 在远程结账时，银行和收款方进行可证连接（略）；

2. 银行进行验证并结账

3. 银行向收款方发出结账通知。

收据事件是在收款方和付款方之间发生。

1. 如果是远程通信，则进行可证连接（略）
2. 收方开出收据，包括：商号（firm）真实性证明和金额真实性证明。

SIG*firm*(time)=(*s*1,*c*1)=sign1

SIG*firm*(amount)=(*s*2,*c*2)=sign2

**虚拟办公网（Office-net）:** 是在文件创建人和文件的阅读人之间形成虚拟链接的可证逻辑网络，提供创建人真实性证明和文件真实性证明，供阅读人用于是否打开文件，是否采信的依据。文件的加密分存储加密或传送加密。存储文件用阅读者自己的公钥加密，而传送文件用对方公钥加密。

由创建人提供：

SIG*creator*(time)=(*s*1,*c*1)=sign1

SIG*creator*(data)=(*s*1,*c*1)=sign2

如果文件需要加密，则：

*r*G=key

Ekey(data)=code

ENC*READER*(key)=β

msg={code，β}

如果文件时加了密的，那阅读者首先进行脱密（只有指定的阅读者才能脱密）：

DNC*reader*(β)=key

Dkey(code)=data

由阅读人检查创建人的真实性，对打开文件与否做出决定：

VER*CREATOR*(time,*s*1)=*c*1’

由阅读人检查文件的真实性，对读不读文件做出决定：

VER*CREATOR*(data,*s*2)=*c*2’

**7网际安全**

通过多年的摸索和发展，对物联网属性逐步有了比较清晰的理解：实体安全的本质是“实体”真实性的证明，证明的出发点是“互相怀疑”；证明的目的是为了实施自主可控策略；证明的方法是基于证据的当场证明；证明的实现是数学方法的正面证明与反面验证，其数学方法是基于标识的公钥体制。物联网在实体之间构成平面格状化可证网络，必须解决鉴别所用私钥的规模化的分发。

如果孤立的实体构成物联网，那么，实体和实体之间就构成事联网。物联网和事联网都是虚拟网络，事联网有些像量子纠缠。量子纠缠是在两个量子之间发生相同的反应，即对等物理现象；而在事联网中，一端实体发生的正过程，在另一端实体中则产生逆过程，这就是证明过程和验证过程，即不对等逻辑现象。事联网在事件之间构成平面的格状化可证网络。事联网包括很多不同类型、不同业务范畴的事件，即包括了很多虚拟网。在不同事件之间形成复杂的链接关系，但是将事联网分解成独立的虚拟网时，很容易找到解决方案。如果物联网中的任意实体，均能被证明或验证其真实性；如果事联网中的任何事件，也均能被证明其真实性，那么我们就可以说，这就是总体安全的最终解决方案。

事件有单一事件、关联事件、复合事件。如果能够把关联事件和复合事件有机地分类为单一事件，安全性证明就变得简单易行。事件的鉴别是以分类学为基础的，因此对事件的分类问题在安全性证明中，特别是在总体解决方案的设计中占有非常重要的地位。

对实体、对事件鉴别的目的是为了实现自主可控。自主可控是新型网际空间中的新的安全原则，应从传统的他主可控（强制控制）的模式中解脱出来。

对实体、对事件真实性证明方法应是基于证据的证明，应从传统的基于信任或基于模型的证明模式中解脱出来，在远程鉴别中禁止使用对称性口令。

对实体、对事件真实性证明应该是“当场证明”，阻断任何信任的转移，应从传统的登录机制中解脱出来，防止权力被接管。

一个网际空间包括很多不同类型的实体，处理不同类型的事件。如何合理处理不同实体和不同事件的鉴别问题，必然涉及到密钥管理问题。密钥管理的好坏直接关系到鉴别系统的好坏。因此密钥管理将成为重点研究的专题。在CPK鉴别系统中提供经常使用的实体名，如：通信标识，发送者标识包括因特网用户名、电话网手机号码等；又如交易标识，包括账户、卡号、票据发行行等；如防伪标识，包括厂家和软件发行企业名；提供身份标识，包括这是姓名，身份号等；因此，标识到标识的（I to I）虚拟谅解是物联网物联网的基本连接方式，而万物就是实体和事件构成，只要解决实体鉴别和事件鉴别，就可以说解决了网际空间的基本安全。

**小结**

基于“I to I”鉴别模式构建自主可控系统是网际安全的核心。自主可控理论将被动防护的安全策略转变为主动管理的策略；将基于信任的“可信系统”转变为基于证据的“可证系统”；虚拟化理论将形象化思维模式转变为抽象化的思维模式，使我们将复杂的网际安全问题得以简单解决。

CPK组合公钥，从2003年正式公布到现在经历了十多年的风风雨雨，最终形成了能够抗击量子计算攻击的体制。CPK系统受磨难的过程，在一定程度上反映了我国网际安全发展的真实情况，也暴露了很多存在的问题。幸好，CPK正冲出十年被冷落的局面，走进缓缓点燃星火的新局面。一个新理论、新概念、新技术被人们深入了解是需要过程的，争论是必须的。但是必须警惕学术领域中的宗派主义倾向，利益集团中的排他主义倾向。

网络世界的主要威胁将是恐怖活动。目前陆地上的流血的恐怖活动，会转入不流血的网络恐怖活动，战场最大可能是金融系统。因此，防止恐怖活动，无论是陆上流血的恐怖活动或网络上不流血的恐怖活动，是全人类共同的责任。

构建自主可控网际安全是庞大的系统工程，需要全人类的共同合作，需要共同维护人类命运共同体。