计算机科学 2005Vol. 32№. 11

机器可读旅行文档的安全分析*)

朱新山　高　勇　王阳生

(中科院自动化所　三星综合技术院人机交互联合实验室　北京 100080)

摘　要　新一代通关检测系统使用了生物特征认证技术。而含有生物特征信息的机器可读旅行文档(Mrtds)的安全是一个极为重要的问题。本文中我们首先分析了对 Mrtds 中机器可读区数据的潜在威胁。然后总结了由国际民航组织(ICAO)推荐的系统安全方案,也就是基于公钥体系的数字签名。基于这些内容,我们把 Mrtds 的认证过程看作是被保护数据,相应的 hash 值和数字签名以及持有者共四个环节之间的连接。对于用于每个连接中的技术,也就是公钥体系,数字签名和生物认证技术,我们提出了一些附加的要求和安全特征。结果,改进的系统加固了每个连接,从而获得了更高的系统安全性。

关键词　机器可读旅行文档,公钥体系,数字签名,生物特征认证

Analysis of the Security of Machine Readable Travel Documents

ZHU Xin-Shan　GAO Yong　WANG Yang-Sheng

(CASIA-SAIT HCI Joint Lab, Institute of Automation, Chinese Academy of Sciences, Beijing 100080)

Abstract　The new authentication system adopts biometric verification technologies. And the security of Mrtds with biometric information is an extremely important problem. In this paper, we first analyze the implicit menaces to data of machine readable zone in Mrtds and conclude the suggested system security scheme, i. e., PKI digital signature by ICAO. Based on these, we consider the authentication of Mrtds as the links among the following four elements: the protected data, the corresponding hash value and digital signature, and the holder. To the technologies used in each link that is PKI, digital signature and biometrics, we propose some additional requirements and security characters. So that the improved system reinforces each link in the system and the greater system security level is reached.

Keywords　Mrtds, Public key infrastructure, Digital signature, Biometric verification

1　引言

为了提升国际安全,ICAO 的最新标准规定用于身份识别的 Mrtds(包括护照和签证)必须含有人的生物特征数据。通过现场采集 Mrtds 持有者的特征数据并与 Mrtds 上的相应数据做匹配来确定 Mrtds 持有者的真实身份。此种匹配由计算机辅助完成,因此大大提升了通关的速度和 Mrtds 自身的安全性。

然而,新通关系统的实现会牵涉到多方面与安全相关的问题。其中包括生产和制作环节中,像材料和工艺的选择,打印技术的选择,与安全生产相关的管理和保密措施;选择什么样的介质存储必要的个人数据;如何鉴定数据的完整性和真实性;如何防止私有数据(象关键的密钥)的泄漏等等。ICAO 为此制定了一系列标准和技术建议,如表 1 所示。

由于系统安全工作庞杂,在此我们仅考虑了如何巩固和提升 MRZ(机器可读区)数据的安全性,为此提供了一些措施和技术建议。

表 1　Mrtds 安全技术文档

标　准	内　容
ICAO Doc 9303, Part 1	机器可读护照的安全标准
ICAO Doc 9303, Part 2	机器可读签证的安全标准
ICAO Doc 9303, Part 3	Mrtds 的尺寸规定
文献[1]	基于 PKI 体系的数字签名方案
文献[2]	Mrtds 机器可读区的逻辑数据结构

2　安全的主要威胁

当然,考虑安全问题首先应该明确的是系统潜在的威胁和挑战。Mrtds 中 MRZ 数据将会面对下面四种主要的威胁[ICAO Doc 9303, Part 1]:

(1) 完全伪造一个 Mrtds

(2) 删除部分 MRZ 数据

(3) 更改部分 MRZ 数据

(4) 冒名顶替者(比如说整容了的)

其中,(1)和(3)表征 MRZ 数据的真实性;(2)表征 MRZ 数据的完整性;(4)表征生物特征识别算法的有效性,也就是能否可靠地将人和 Mrtds 连接在一起。

3　安全的基本准则

ICAO 的标准里描述了用于保护 Mrtds 机器可读区内逻辑数据结构的一些准则,以使被授权的接收组织和接收州能够正确地读取和可靠验证这些信息的真实性和完整性。这些准则包括[2]:

- 某种安全的钥匙必须在各州之间分发用来验证 Mrtds 数据的真实性和完整性。
- 所使用的安全技术广为人知而且全球都可以接受。
- MRZ 数据的完整性必须能够证实。
- MRZ 数据的真实性必须能够证实。
- 在 Mrtds 制作时,发布州或组织应该输入用于检测数据完整性和真实性的信息。

*)课题得到自然基金项目(60473047)资助。朱新山　博士研究生,主要研究方向为隐藏与信息安全。高　勇　博士研究生,主要研究方向为计算机视觉。王阳生　研究员,博士生导师,主要研究方向为计算机视觉。

• 要保存的用于验证的信息必须很少。

• Mrtds 的发布者应该限制接收州使用一些生物特征数据或显示数据。这些数据应该被加密以阻止访问。

因为这些准则是安全性所必需的，所以所提出的方案应该遵循这些准则。

4 基于 PKI 体系的数字签名

ICAO 的标准中提出应用基于 PKI 体系的数字签名来验证 MRZ 数据的真实性和完整性。它的主要思想是使用 PKI 体系来加密 MRZ 数据及其相应的 hash 值，并生成一个相应的发布州的数字签名。这些信息被一同存储到 Mrtds 的机器可读区，其结构可参考文档[2]。因为签名根据发布州的私钥获得，它不可能被伪造，从而通过验证数字签名可以证明数据的真实性，即此数据确实来自发布州。数据的完整性是通过对比 hash 值是否相同来验证的，见图 1[7]。这两个过程都要使用发布州的公钥，因此公钥的发布和更新是整个系统安全的重要方面。为此，ICAO 提出了一个 PKI 体系。

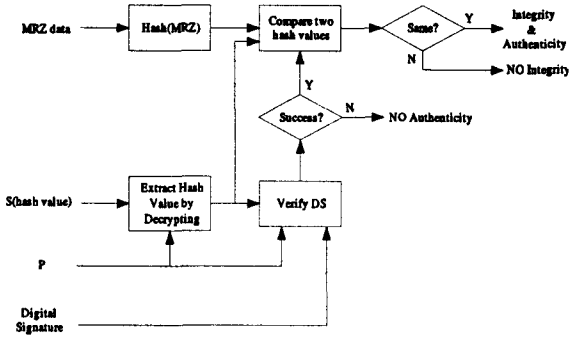

图 1 MRZ 数据真实性和完整性的验证

4.1 系统结构

如图 2 所示，本系统被分为三个层次。最高一层为 ICAO，其次国家的中心节点，最后是各个州一级节点。通关检测将会在州一级进行。

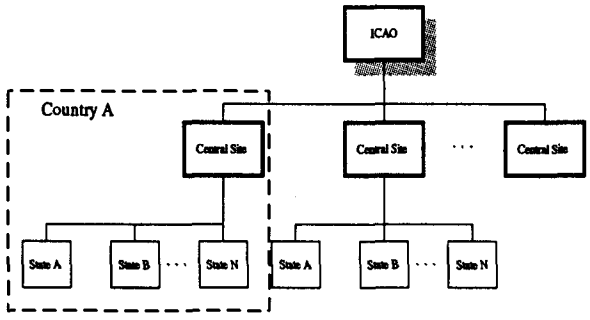

图 2 应用于 Mrtds 的 PKI 体系结构

4.2 中心节点

每个国家内部只允许有一个中心节点，他负责密钥的生成和管理，如图 3 所示。其功能概括为：

• 负责为它下面的每一个州（即州一级节点）都生成一对密钥，即私钥和公钥。

• 为其自身生成一个根钥和另一对密钥专用于发布公钥时生成国家的签名。

• 为每个州要申请的 Mrtds 计算数字签名。如图 4 是一个基本的 Mrtds 的签名过程。

• 管理私钥和发布公钥。

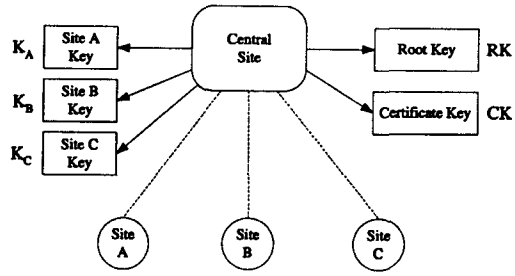

图 3 中心节点产生密钥

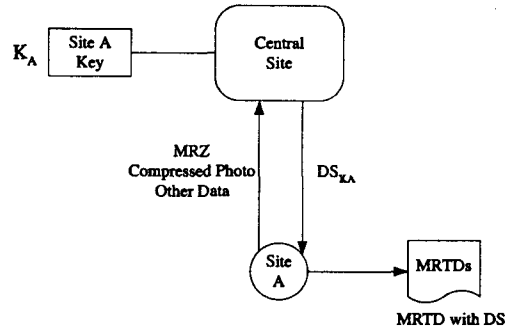

图 4 由中心节点为申请注册的 Mrtds 计算数字签名

4.3 ICAO

ICAO 负责建立一个公钥查询目录，即 PKD，它唯一的功能就是保证接收州能够及时准确地获得通关检测中所需要的公钥。ICAO 搜集各个国家所发布的公钥的信息，并在证明其正确性后存入 PKD。这种信息的搜集和证明过程是在 ICAO 和各个国家的中心节点之间进行的。它由三步完成，即数据传输、证实和再传输，如图 5 所示。

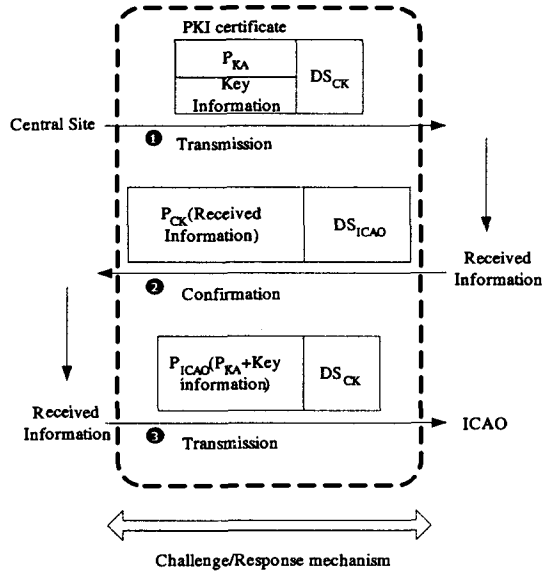

图 5 在 ICAO 处更新每个州的公钥

5 建立更安全的系统

一个系统的安全水平取决于这个系统中安全性最低的那个环节，这是我们在考虑安全问题时应该牢记的一个基本原则。从上面 ICAO 提供的标准里，我们可以看出新的 Mrtds 的验证过程涉及如图 6 所示的几个环节[3]。要保证各个环节连接牢固可靠，就必须做到如下几点：

·严格保密私钥;

·正确获得公钥;

·采用安全的算法,包括加密,数字签名和 hash 函数,并且在 Mrtds 验证中严格采用由发布州指定的算法;

·研究可靠的生物特征识别算法。

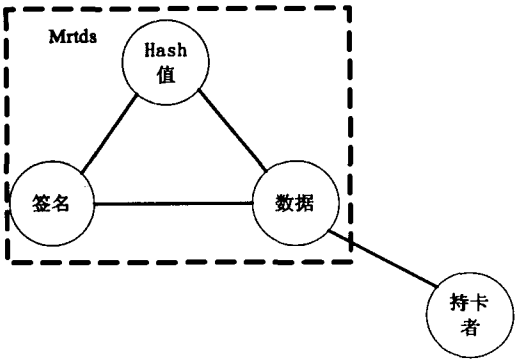

图 6 Mrtds 验证过程中各环节的关系

5.1 私钥的安全

在上一节中可以看到各个州的钥匙对都是由它所在国家的中心节点产生。其中所有的私钥都是保密的,任何组织无权访问。保护私钥的安全是整个系统安全的关键。所以中心节点必须是一个安全的节点。为此,ICAO 建议使用带有合适输入控制的硬件安全模块(HSM),如图 7 所示。我们认为建设安全的中心节点要考虑的问题包括:

·由物理的和电子的设备来保护私钥;

·有严格的访问控制和安全的更新机制;

·能快速签名而不泄漏私钥;

·尽量和公共网络隔离,严防黑客的攻击,对不明身份人侵者要设置报警系统。

由于私钥的保护只在中心站点,许多技术可以使用,能够做到尽量的安全。

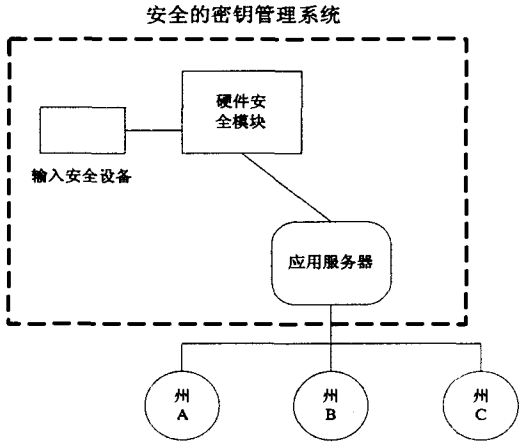

图 7 国家内中心节点的结构

5.2 获得正确的公钥

公钥虽然是公开的,但是它的安全性也需要保证。其体现在,接收州能及时正确地获得发布州的公钥。由于接收州获得公钥的方式就是查询 ICAO 的 PKD 目录,为达到上述目的,ICAO 要做到如下几点:

(1)从发布州获得正确的公钥;

(2)存储在 PKD 内的公钥不能被更改;

(3)要及时通知世界上所有的州,哪些州的公钥被更新了。

通过 4.3 节所提到的数据传输、证实和再传输这一过程,(1)能够实现;(2)实际上要求 PKD 也是一个安全的站点。由于这些公钥并不要求保密,只须证明其正确性就可以,因此 ICAO 在 PKD 里除了存储公钥以外,还附加了 ICAO 的签名和发布此公钥的国家的数字签名,用来证明公钥的真实性。此数据结构如图 8 所示。为实现(3),ICAO 在获得新的公钥信息以后应该立即通知所有州,这是个自动的过程。另外,还要求 ICAO 在 PKD 中存储公钥的一些信息,像使用期限。

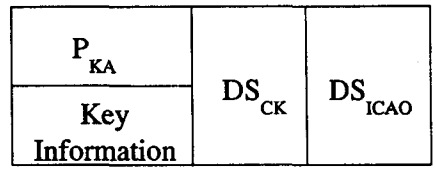

图 8 PKD 内的数据结构图

5.3 安全高效的 PKI 算法

很明显,选用的 PKI 算法和密钥的长度与整个系统的安全息息相关。另外,在实际问题中,加密和解密的速度也必须考虑。下面我们来比较一下几种流行的 PKI 算法,如表 2 所示[1]。

表 2 PKI 算法性能比较

算 法	ECDSA	DSA	RSA
算法 ID	01	02	03
签名钥匙(私钥)长度(字节)	20(160 bits)	20(160 bits)	256(2048 bits)
相对签名速度	Fast	Medium	Slow
签名尺寸(字节)	40(320 bits)	40(320 bits)	128(1024 bits)
验证钥匙(公钥)长度(字节)	21(161 bits)	128(1024 bits)	136(1088 bits)
相对验证速度	Medium	Slow	Fast

从表 2 可以看出,如果 Mrtds 的存储空间有限,我们可以考虑采用 ECDSA 算法。因为其验证速度中等,比较合理,公钥和私钥长度都小(达到安全性至少需要 161 位和 160 位,此时生成的数字签名仅有 320 位,节省了 Mrtds 的存储空间。)相反如果存储空间不是问题,RSA 是更好的选择。因为它验证速度快,要达到安全性至少需要的私钥长度是 2048 位,此时生成 1024 位的数字签名和需要 1088 位公钥。

另外,hash 算法默认使用 SHA-1,这样避免了在 Mrtds 的 LDS 里再指定所使用的 hash 算法。对 SHA 还没有已知的密码攻击,并也由于它产生 160 位散列,因此它更能抵抗穷举攻击。

在能保证私钥安全,公钥正确获得情况下,通关安全的实现还必须保证在 Mrtds 验证过程中采用由发布州所指定的 PKI 算法,因为有可能的攻击是 Mrtds 所指定的 PKI 算法的 ID 被更改了。

5.4 数据存储器

数据的安全性还与所使用的存储器自身有很大的关系。一方面是存储器的容量,大容量的存储器可以容纳更多的附加数据用于维护关键数据的安全;一方面是存储器所使用的技术,比如二维条码、智能卡技术。现在智能卡技术日臻完善,它与 PKI 体系的结合大大提升了系统安全。它自带

CPU,可以在其内部作各种数据操作;自身有严格的读写控制系统,可以有效地防止不合法的用户更改数据。当然,它也有自身的缺陷,因此要求我们在存入数据前数据应进行加密,并且我们的产品必须来自可信度高的厂家。我们推荐使用智能卡技术,它相当于在我们数据的外围再增加一个物理保护设备。智能卡还可以提供双向鉴定技术,这可以防止不合法用户随意访问智能卡,阻止克隆,间谍等攻击,比 ICAO 所提出的单向鉴定方案更加安全。

5.5 隐藏秘密的信息

上面我们讨论的 Mrtds 逻辑数据区内(LDS)的数据都是可访问的。然而,LDS 的设计还预留了一些数据区给发布州使用,例如 LDS 中的第 5 和第 15 号可选数据区[1]。因为,可访问的信息容易成为攻击的目标,所以在预留区内放置一些秘密信息是有利于系统安全的。使用秘密的信息,我们可以达到两个目的:1)作为专家级鉴别和法庭鉴别 Mrtds 真伪的一个手段,可以提供毫不含糊的证据;2)进一步防止非法机构伪造 Mrtds,因为它无法获得这些秘密信息。为保护这些数据的安全性,我们建议:

- 采用非标准的加密算法;
- 严格控制对密钥的访问权;
- 解密过程只在智能卡内进行,此数据不能读出。

除了 LDS,在 Mrtds 的可视区,像文字,背景图片等,还可以通过数字水印技术隐藏一些秘密的信息用于验证 Mrtds 的真伪。它的优点是不容易引起注意,从而招致恶意的攻击。此种应用要求数字水印技术能够抵抗一轮打印扫描的攻击。在设计具体算法时可参考保护文档的水印文[4]和用于印刷品防伪的文[5]。

5.6 生物特征识别技术的要求

新的 Mrtds 对个人身份的认证采用的是生物特征识别技术。而生物识别技术不能像密码体系那样提供等价的验证。检测的精度依赖于这些技术的性能指标。

(1)错误接收率/错误拒绝率

对于此系统接收一个持有 Mrtds 的冒名顶替者和拒绝一个真正的 Mrtds 的持有者是同等重要的。这两个错误率不能高于 10%的系统在实际中才能工作。

(2)算法的复杂度

如果算法复杂度小,验证过程可以在智能卡内部一对一地进行。智能卡可以提供足够的计算资源和存储空间,验证的速度也会加快。

(3)算法对伪造的身份要敏感

这一点是在选择生物特征识别技术算法时必须考虑的。例如:人的指纹特征容易伪造,因为指纹是公开的;虹膜图片对光线敏感。应对这类攻击的方法是 1) 使用多种生物特征,像两个以上;2)提升生物特征传感器对伪造特征的识别能力,比如说使用指纹温度采集仪和人脸红外线采集仪等。

(4)采用人们容易接受的生物特征

比如说人脸,指纹,声音数据都是公开的,容易被人接受;但是,像人手血管和 DNA 的数据就是私人的了。另外,还有一些技术可比较危险,像虹膜检测。

在实际测试中,依赖于单一生物特征的认证系统常常不能可靠地工作。这是由它们固有的问题所决定的,像人脸识别对光线条件特别敏感[6]。一种有效的解决方案是采用多种生物特征相融合的技术。文[7]显示使用信息融合能够提升多生物特征检测系统的性能。目前,中科院自动化所研制的通关系统,融合了人脸识别、指纹识别和虹膜识别。全部完成三种检测,仅需 13 秒,大大提升了通关的速度。但是,在这个系统中应用优秀的融合算法还在进一步探索中。

总结 基于生物特征识别的通关检测系统,已经提上应用的日程。而如何保护 Mrtds 的安全是一个复杂的工程体系。上述安全方案从物理设施到具体算法,从管理到软件实现,形成了一个层级式的抵抗威胁的系统。这为设计安全的 Mrtds 系统提供了具体的技术指引。

参 考 文 献

1 PKI Digital Signatures for Machine Readable Travel Documents:[Technical Report]. ICAO/TAG NTWG, v. 4, 19/04/2003
2 Development of a Logical Data Structure - LDS for Optional Capacity Expansion Technologies: [Technical Report]. ICAO, Draft v. 3, 31/10/2003
3 Schultz J F. Enhanced security proposal concerning the electronic Passport specification issued by the ICAO: [Technical Report]. ICAO, Draft v. 0.5, 11/02/2004
4 Brassil JT, et al. Copyright Protection for the Electronic Distributionof Text Documents. In: Proc. of the IEEE
5 宋玉杰. 数字水印及其在印刷品防伪中的应用:[博士学位论文]. 北京:中国科学院自动化研究所,2002
6 Wang Haitao, Wang Yangsheng. Recognizing Face Images Under Different Lighting Conditions. In: IEEE Intl. Conf. on Acoustic, Speech and Signal Processing (ICASSP), Hong Kong, 2003
7 Ross A, Jain A K. Information Fusion in Biometrics. Pattern Recognition, 2003, 24(13): 2115~2125
8 Schneier B. Applied Cryptography. Second edition. New York, et al: John Wiley & Son, Iinc., 1996