

About ZerOne (From 2006)



微信圈里晒登机牌的常见姿势



登机牌票面结构

1 24小时订票专线 96780 机场贵宾 芳龄俱乐部 登机牌

Name: [Redacted] Seat: 51C
Flight No: MF8244 Class: R
Destination: HGH (杭州) Gate: 8
Date: 08NOV Departure Time: 2045
ET 11 51C
08NOV
086 ET
CWAG

13

NOTICE: GATE WILL BE CLOSED 10 MINUTES BEFORE DEPARTURE.

需要注意的是

ETKT 13-14位数字：电子客票旅客客票号，前3位是航空公司编码，后10位是客票号码，第14位是安全码（非必需）

NI，后跟身份证号

关于API与PNR

- **PNR**

- **Passenger Name Record 旅客姓名记录/旅客订座记录**
- **是指航空器运营人或其代理为每名预期旅客的每项订座所建记录而起的通用名称。**
- **内容包括护照、签证以及前往城市的住址等信息**

- **API**

- **旅客预报信息**

- **2012年9月，蒙特利尔，高级别航空保安会议（HLCAS）中，在议程项目7：“旅客姓名记录（PNR）数据及其在航空保安方面的作用”工作文件中，明确指出DOC9944文件的来由和主要功能。**

关于DOC 9944号文件

- 2010年，国际民航组织出版了经修订的指导方针，作为《关于旅客姓名记录数据的指导方针》（即Doc9944号文件）

国内登机牌解析—东航



对应代码如上

| | |
|---------------------|-----------------------------|
| FM9364 24 1D WUH005 | |
| - FM | IATA二字代码，FM即上海航空股份有限公司（中国）。 |
| - 9364 | 航班号。 |
| - 24 | 当月的日期，只显示月日中的日。 |
| - 1D | 座位号。 |
| - WUH | 始发地城市三字代码，WUH对应为武汉。 |
| - 005 | 顺序号，即第5个办理Check-in的旅客。 |

国外登机牌解析—美联航



01623389961491

M15MITE/JOHN MR DXAIGR YCYVRWS (P53 006Y004D0001 100)

国外登机牌解析--加拿大西捷航空

WEST JET BOARDING PASS / CARTE D'EMBARQUEMENT SMITH/JOHN MR
06 JAN 12 0553 GATE GATE GATE / PRE GATE
SMITH/JOHN MR SEQ 001
DEP CALGARY INTL AB 6:00PM TIME 05A 000
ARR VANCOUVER BC 6:20PM
TERMINAL / BOARDING TIME / SEAT / PLACE
AEROSLANT / HEURE D'EMBARQUEMENT / SEAT / PLACE
MAIN 5:30PM 4D 4D
ELECTRONIC TICKET NUMBER
81821775464477



座位号如此

M1SMITH/JOHN MR DXAIGR YYC YVRWS 0553 006Y004D00001 100

国外登机牌解析—美国航空公司

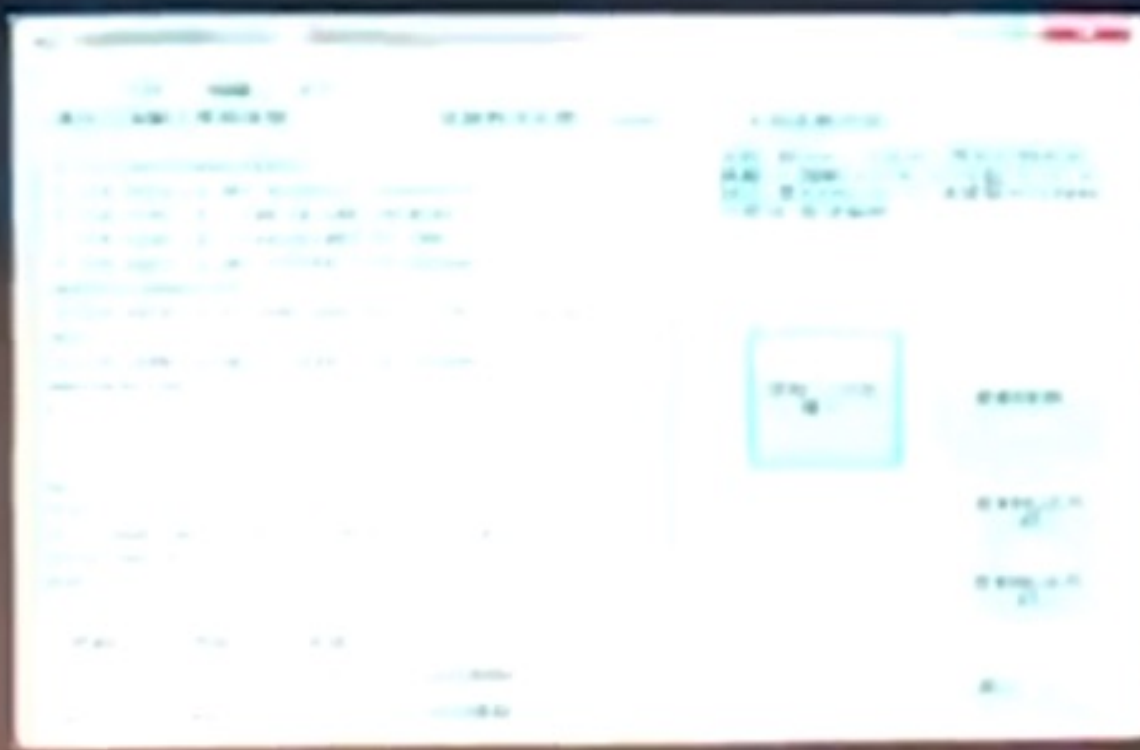


0011805241606

MIWAKEFIELD/DARRIN MR 100PCPW ORDIANAA 2517 299A001R0020
11B-10B 0299BAA 290011605/416060 AA 01 01 * 8500 8

隐患泄露风险1：通过PNR跟踪乘客信息

- 恶意的攻击者依然可以通过PNR来跟踪乘客的行程信息
 - 随机同行的人员清单
 - 订购者私人信息等。
- **攻击者可以借此实现：**
 - 提前换取登机牌
 - 读取行李票号
 - 偷窃他人登机牌
 - 人为劫持登机牌等。



PNR信息

1. MFJDOWN
2. KN5927 V SA21MAR NAYXMN RR1 0710 0955 E--T4
3. T SHA/SHA/T-021-34064880-454360/SHA HUA CHENG SOUTHWEST TRA
4. T SHA/VEL/SHAO/JI HONG
5. SSR FOID KN HK1 NI110108201 247/P1
6. SSR TKNE KN HK1 NAYXMN 5927 V21MAR 7818581172025/1/P1
7. SSR CHLD KN HK1 06NOV11/P1
8. OSI CA CTC 021-51069999X454360
9. OSI KN CTCT180 37
10. OSI CA TKNA TICKED
11. PEK1E/JQ2DJ8/SHA713

1. 乘机人姓名与PNR

2. KN5927航班，3月21日，V舱，北京南苑机场-101高崎机场，早07:10起飞，09:55抵达

3. 上海的票务代理 4. 代理人票务的负责人

5. 将身份证信息输入SSR，身份证号持有者是一个4岁的孩子

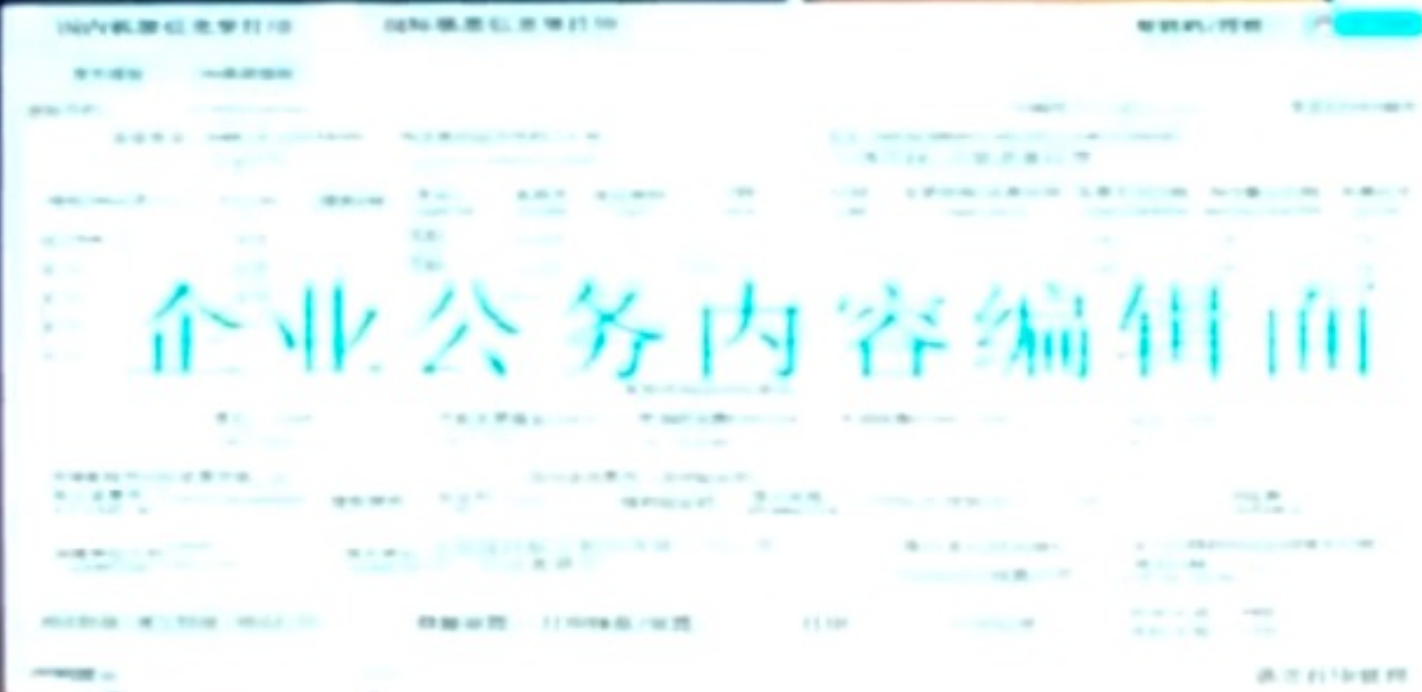
6. 重复2内容，并生成电子票号为7818581172025

7. 统一儿童票预订格式 8. 订座时预留座机号码

9. 订座时强制要求输入联系人手机号，即乘机人手机号码。

伪造登机牌

- 地下产业链
 - 白牌批发
 - 登机牌制作

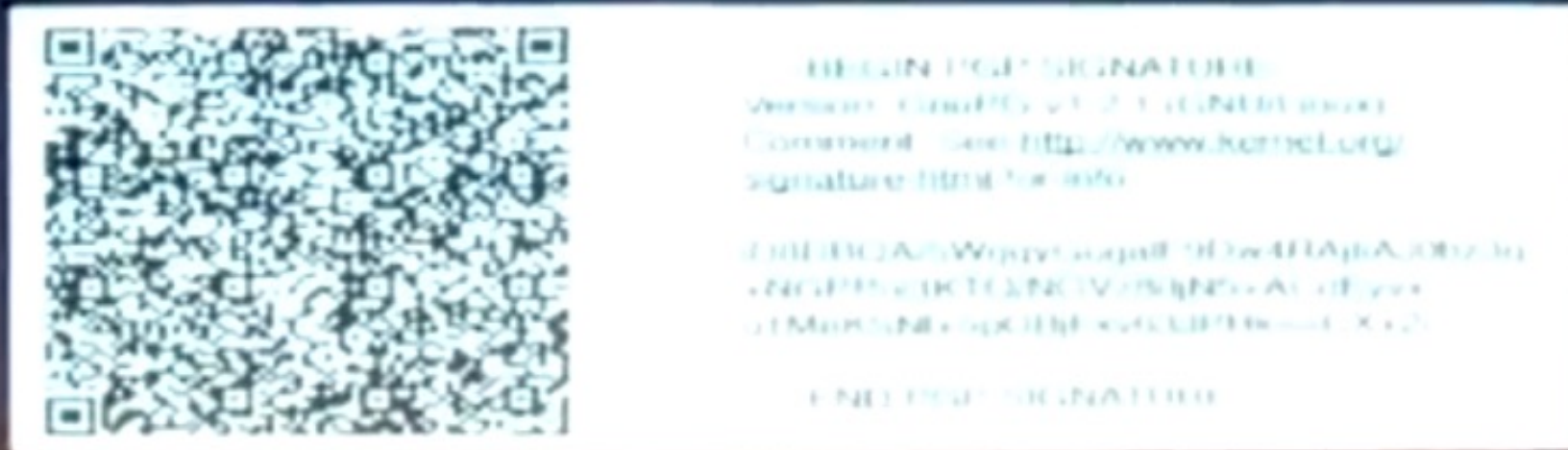


伪造登机牌难度

| 序号 | 航空公司 | 航班号 | 始发地 | 日期 | 座位 | 登机牌一维Hash | 伪造难易 |
|----|------|---------|---------|----------|-----|---------------------|------|
| 01 | 南航 | CZ6594 | HGH杭州 | 201X0708 | 23C | CZ6594 0823CHGH051 | 存在风险 |
| 02 | 东航 | MU2116 | PEK北京 | 201X0214 | 84B | MU2116 1484BPEK097 | 存在风险 |
| 03 | 国航 | CA1368 | SZX深圳 | 201X0730 | 311 | CA1368 30311JSZX125 | 存在风险 |
| 04 | 深航 | ZH99836 | CTU成都 | 201X0216 | 26F | ZH99836 1626FCTU094 | 存在风险 |
| 05 | 海航 | HU7823 | XIV西安 | 201X0624 | 32E | HU7823 2432FXIV059 | 存在风险 |
| 06 | 吉祥 | HO1217 | SHA上海 | 201X1210 | 23E | HO1217 1023ESHA143 | 存在风险 |
| 07 | 西部 | JD5401 | XIV西安 | 201X0923 | 70E | JD5401 2370FXIV122 | 存在风险 |
| 08 | 川航 | 3U8588 | URC乌鲁木齐 | 201X0522 | 17H | 3U8803 2277HURCD90 | 存在风险 |
| 09 | 昆明 | KYR238 | KMG昆明 | 201X0912 | 24E | KYR238 1224EKMG102 | 存在风险 |
| 10 | 厦航 | GJ8697 | HGH杭州 | 201X0611 | 10E | GJ8697 1140XHG017 | 存在风险 |

强化措施：PGP签名QR二维码

- 基于PGP签名技术的QR二维码，可以更加有效地加强登机牌的安全性



NFC Boarding Pass



Boarding a flight with an NFC instead

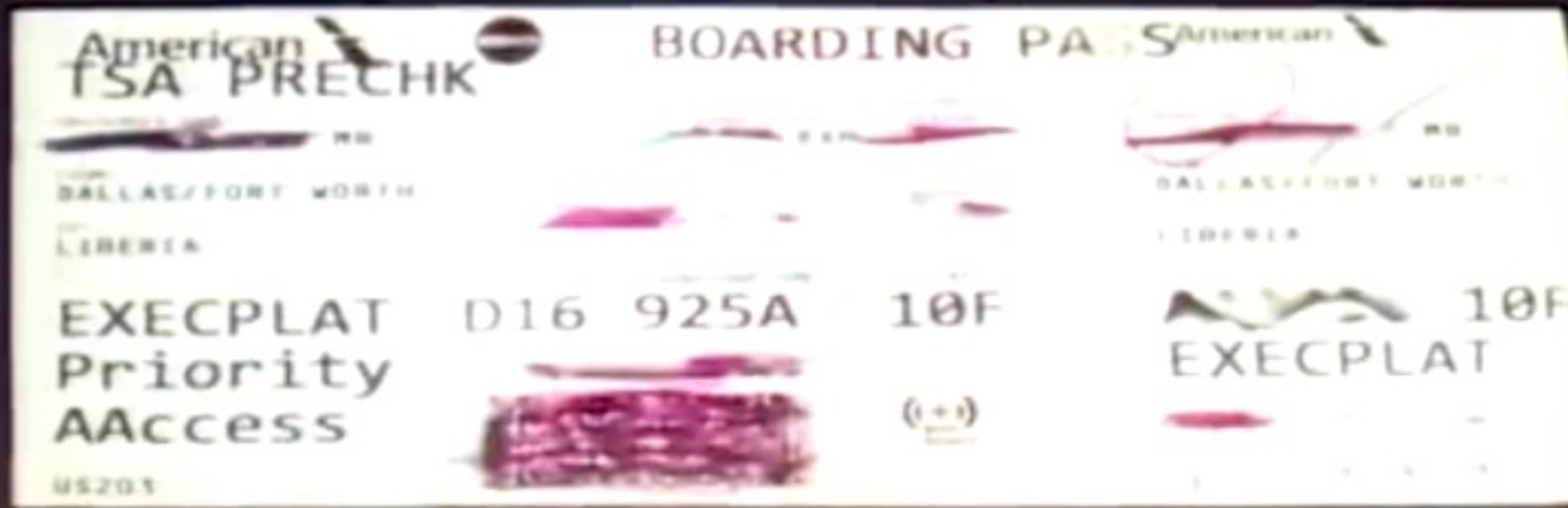


Forensic && Count-Terrorism

- 现勘/取证/事件还原
- 反恐需求
 - 911事件残骸
 - DNA+登机牌+其它资料
 - 确认嫌疑人身份



如何处理登机牌？





杨哲

ZerOne

Wireless Security Research

(Longas)

ZerOne 无线安全研究组织



Thanks !!

Hack Inn

一个收集分享国内外安全会议资料的网站，
我们认为每一份议题都值得留传。

<https://www.hackinn.com/> 联系邮箱：admin@hackinn.com