September 21, 2005
AUD 06-A0002

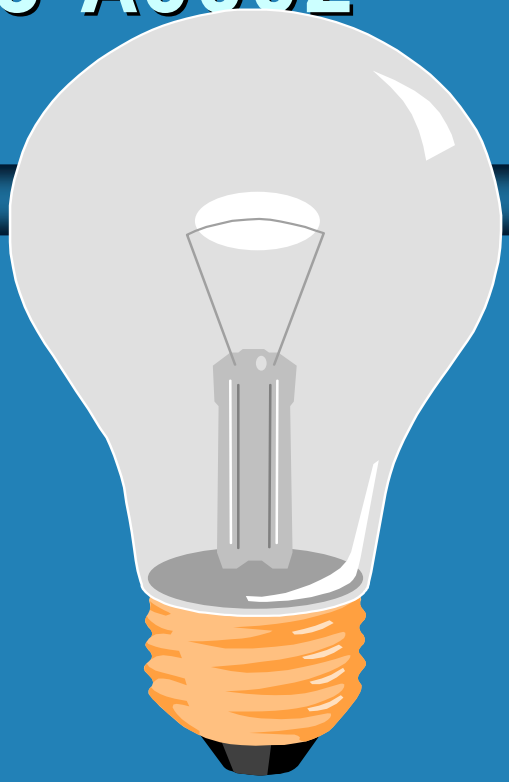
Office of Auditor General Internal Audit Advisory Report

Review of Visa Debit Card Security

Office of Auditor General

Internal Audit Advisory Report No. AUD 06-A0002

- Questions



- If you have any questions or comments pertaining to this Internal Audit Advisory
- Report , please contact:
- James C Stewart 962-1008

SUBJECT: Review of Visa Debit Card Security
FROM: AUDT - James C. Stewart

DATE: September 21, 2005
IN REPLY
REFER TO: AUD 06-A0002

TO: TRES - Alvin W. Doehring

Background

WMATA's customers can purchase fare media with debit cards, which requires customers to use their Personal Identification Numbers (PIN) to complete the transaction. PINs have to be protected to safeguard debit card usage at the fare vendors and minimize any liability that might occur as a result of unauthorized PIN use. Therefore, PINs are encrypted to prevent attacks on them when customers enter their data in fare vendors.

Visa USA Inc. places tremendous importance on PIN security. Therefore, they have a program that includes on-site reviews to verify that organizations are in compliance with its security requirements. Visa's Operating Regulations require organizations to comply with the Visa Payment Card Industry PIN Security Requirements manual. These requirements help safeguard the Visa payment system and help ensure that organizations are adequately protecting PIN data from compromise. In accordance with the Visa PIN Security Requirements, WMATA is required to submit an annual PIN Security Self-Audit Compliance Statement.

Objectives, Scope and Methodology

The Office of the Treasurer (TRES) requested our assistance in reviewing the WMATA debit card program to determine if WMATA was compliant with Visa's security requirements. There were seven specific control objectives:

- PINS used in transactions are processed using equipment and methodologies that ensure they are kept secure
- Cryptographic keys used for PIN encryption/decryption and related key management are created using processes that ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys
- Keys are conveyed or transmitted in a secure manner
- Key loading to hosts and to PIN entry devices is handled in a secure manner
- Keys are used in a manner that prevents or detects their unauthorized usage
- Keys are administered in a secure manner

- Equipment used to process PINs and keys is managed in a secure manner

The review was conducted in August 2005. We used Visa's PIN Security Program: Auditor's Guide, which was designed to help organizations understand Visa's definition of compliance. We interviewed staff in the Office of Information Technology and Services (ITSV), TRES, Cubic Transportation Corporation and Grace Associates. We also reviewed TRES procedures for Cryptographic Keys and the WMATA PIN Procedure Policy.

The review was performed in accordance with generally accepted government auditing standards and accordingly included a study and evaluation of internal controls and a review of compliance with laws and regulations, as we deemed necessary under the circumstances.

Results of the Review

WMATA needs to address the following issues:

- **PINS processed online did not use Triple DES (Data Encryption Standard) and double or triple length keys.**

- **All cryptographic keys were not created randomly.**

- **Keys should be entered into PIN Entry devices using a secure key transfer system.**

- **ITSV should have a dedicated safe to store key components. Also, a log should be maintained to record when key components are accessed and it should include a witness's signature.**

TRES/ITSV Response to the Review

PINS processed online did not use Triple DES and double or triple length keys

Triple DES is an approved cryptographic algorithm. TRES stated that ITSV would install Base 24 ES software, which would bring WMATA into compliance with Visa's requirements. The software should be installed by February 2006.

All cryptographic keys were not created randomly

Master File Keys (MFK) was created by WMATA to encrypt other keys. The MFK was originally loaded using a manually randomized process. The MFK will change approximately by September 30, 2005 when TRANS 24 software is loaded. The software will use a randomized number generator that is built into the Hardware Security Module. This action will put WMATA in compliance with Visa's requirements.

Another key, the Basic Derivation Key (BDK), which is used to encrypt data between the fare vendors' pin pad units and the WMATA central switch software will also change using a randomized process when WMATA obtains another software product called Base

24 ES. This process should be completed by April 2006.

Keys should be entered into PIN Entry devices using a secure key transfer system
The software used to inject the pin pads was deemed non-compliant by Visa. The software does not use the DES algorithm as required by Visa. However, TRES/ITSV did use dual control and split knowledge when the software they used (Verifone SecureKit) was injected into the pin pads. TRES will research available software that complies with Visa's requirements.

ITSV should have a dedicated safe to store key components
ITSV purchased a safe during the audit to store key components.

ITSV should maintain a log to record when key components are accessed and it should include a witness's signature
ITSV will maintain a log to record when the key components are accessed.

Recommendations:

We recommend the following actions:

1. TRES obtain software compliant with Visa's security requirements that will protect PIN data entered into fare vendors.

2. TRES inform AUDT when TRANS 24 and Base 24 ES software is installed.

James C. Stewart
Auditor General

cc: GMGR – Richard A. White
SCOS - Harold M. Bartlett
CFO – Peter Benjamin
TRES - Edward Barnette
ITSV - Donald P. McCanless