End to End Security of a Transit Ticketing Scheme

An overview of the ITSO security scheme

Tony Breslin / Ian Duthie
Tony.breslin@ecebs.com / ian.duthie@ecebs.com

![e-cebs]

The Heart of ITSO Security

The ISMS – ITSO Security Management System

The ITSO SAM - Secure Access Module [ISAM]

- ➢ The ISAM ensures tickets can be issued, verified and modified securely and relayed securely for settlement

- ➢ The ISAM ensures interoperability and trust between competing Transport Operators

- ➢ The ISAM is the Policeman of ITSO

The ITSO SAM

The ITSO Secure Application Module (ISAM), resides in all ITSO-compliant Point-Of-Service equipment and back offices.
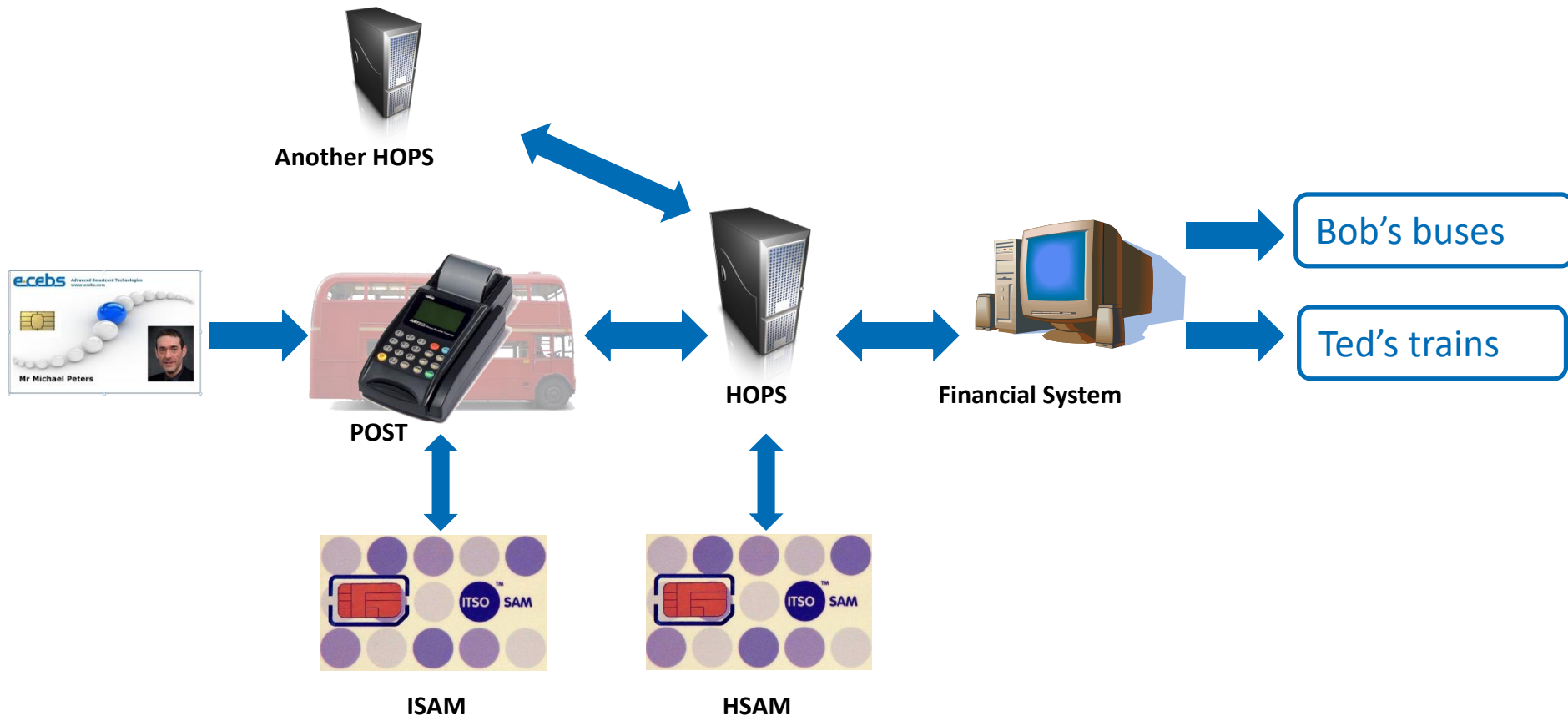

ISAM

ITSO Architecture

❑ ISAMs are used to enforce scheme trust between competing operators by:

- ➢ Verifying and Validating IPEs
- ➢ Securing and optionally storing transactions
- ➢ Verifying Transactions

❑ ISAMs are used to:

- ➢ Create, modify and delete IPEs
- ➢ Support batch management of transactions
- ➢ Support multiple card platforms within the ITSO system
- ➢ At the front office (POST)
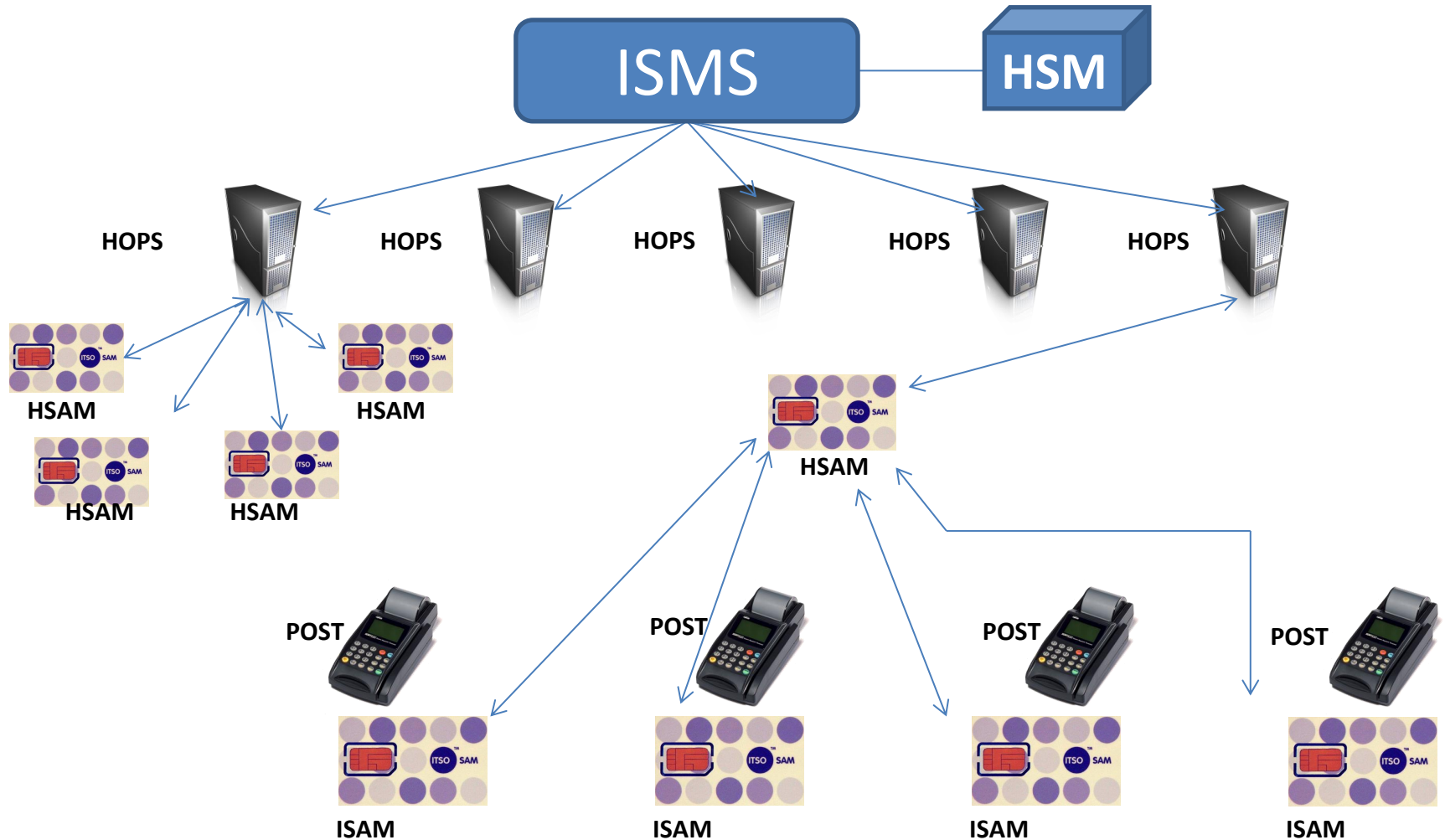- ➢ In the Back Office (HOPS/AMS and HOPS/KMS)

ISAM Functionality

➢ Provides secure key distribution and storage for product management and usage

➢ Allows operators to issue/accept products from a multitude of providers and retailers

➢ Certifies and validates card & transaction data using DES encryption

➢ Provides 8MBytes of secure data storage

➢ Provides a mechanism where all data transactions reach the intended recipient without being 'lost' or tampered

➢ It enforces business rules

ITSO – The Transaction Overview

Another HOPS

Bob's buses

Ted's trains

POST

HOPS

Financial System

ISAM

HSAM

ITSO – The Security Overview

The Future of Transit Fare Collection

ITSO Limitations without Part 11

- Expensive to increase fulfilment points to meet passenger growth e.g. TVM

- Limited fulfilment channels – <u>ISAM must be present and secured in device</u>

- No support for NFC Over The Air download

- Delay (2-48 hours) to fulfil ticket via Action Lists

- Dependency on uncontrollable external systems e.g. HOPS

- Scalability issues

- Nomination of collection area

ITSO Part 11

Without Part 11

Part 11 Client

Part 11 Server

POST

Internet

The Future of Transit Fare Collection
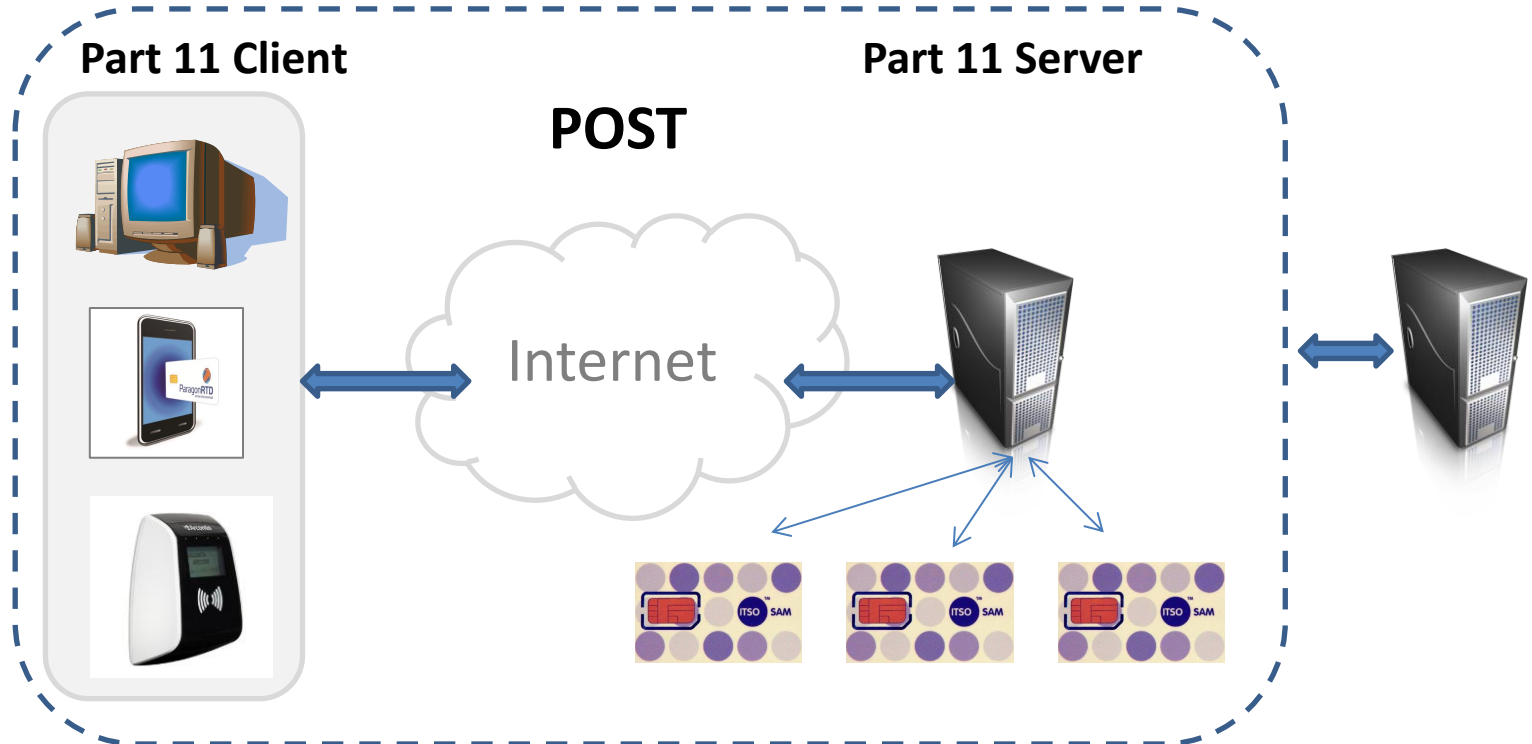
Part 11 – Key Benefits

❑ Increase channels to market away from station and vehicles

❑ Lower cost retail and fulfilment mechanisms

❑ Reduce maintenance costs

❑ Improved customer experience

  ➢ Immediate ticket availability

  ➢ Conveniently collect at any online location

  ➢ Reduce queues at stations and on vehicle

❑ Only solution to support Mobile NFC Over The Air ticket download

❑ Reduce reliance on back office systems e.g. HOPS

ITSO & NFC

Another HOPS

HOPS

Financial System

Bob's buses

Ted's trains

ISAM

HSAM
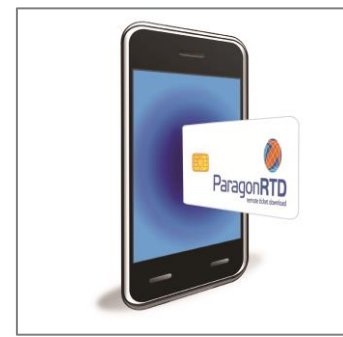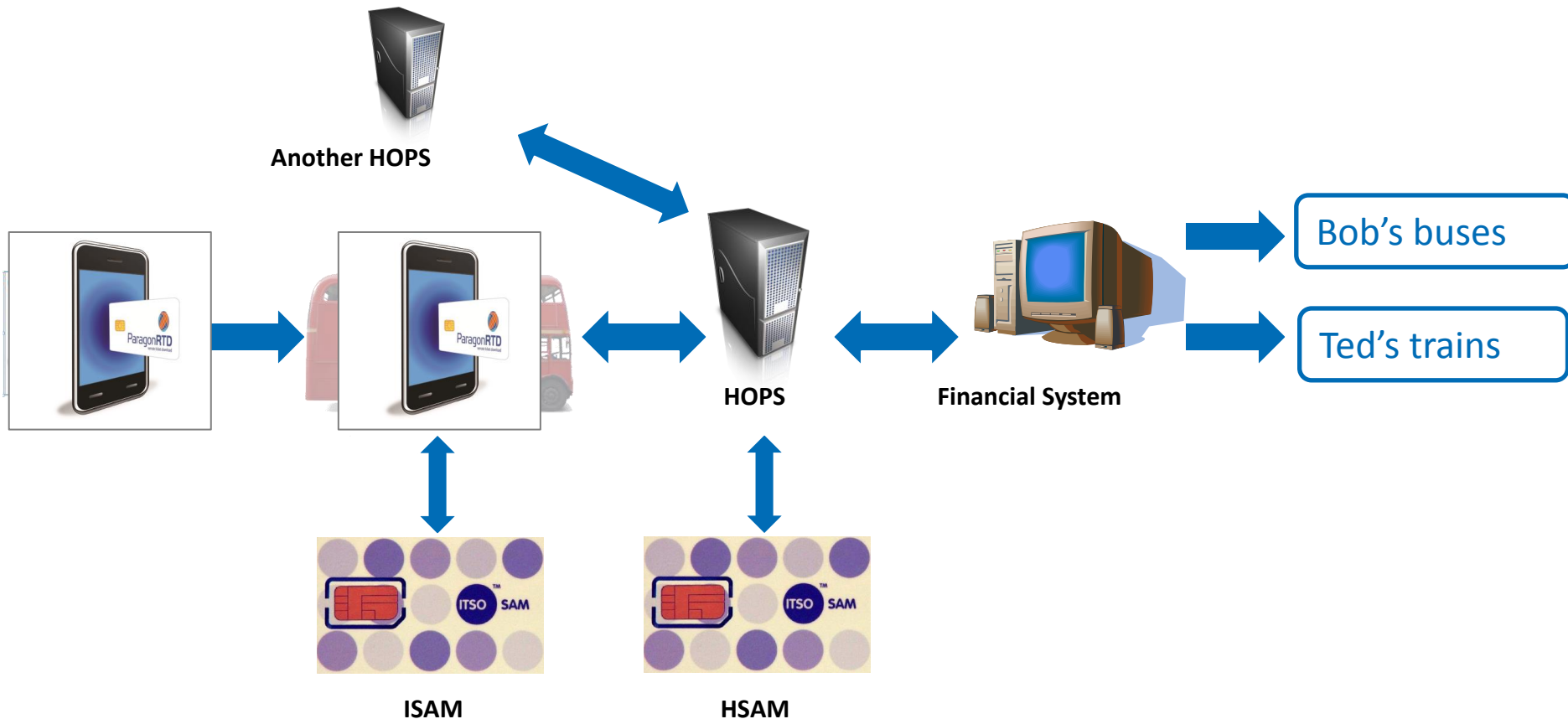
Securing an Open Standard system Summary

❑ An open standard system versus closed system
  ➢ More complex to manage
  ➢ Varied and often independent users
  ➢ More suppliers
  ➢ More variables to manage and secure

❑ Securing an open system
  ➢ Is essential because of the benefits an open system brings
  ➢ ITSO & Ecebs have the experience and proven the technology
  ➢ OSPT & ITSO will enhance this experience
    ▪ Through joint membership alliance
    ▪ Through task force work group

The Future for Transit

❑ Transit Authorities will demand Open Standard Systems

- ➢ For choice of vendors
- ➢ For the security of supply
- ➢ For flexibility of options
- ➢ For future proofing and innovation

❑ The trend will be more and more mobile tickets

- ➢ Pre-loaded by the consumer
- ➢ An improved experience for consumers
- ➢ A cost reduction for the transit authorities
- ➢ **ITSO** & **OSPT** are ready now
  - ▪ And so is **ECEBS**