The CIPURSE open standard for HCE-based ticketing solutions
Welcome to ‘The CIPURSE open standard for HCE-based ticketing solutions’

Your presenters today are:

Laurent Cremer
Executive director, OSPT Alliance

Viktor Brajak
Chairman, HCE Working Group, OSPT Alliance and COO, Medius
Agenda and key learnings

Introducing OSPT Alliance
- Why OSPT Alliance is interested in Host Card Emulation (HCE)
- The OSPT Alliance HCE Working Group

What is HCE
- Why should transport operators consider HCE?

Implementing CIPURSE with HCE
- Why HCE and CIPURSE work so well together
- The best way to implement HCE

Beyond transport ticketing
- Ways to leverage the partnership beyond transport

Conclusions and questions
Introducing OSPT Alliance and CIPURSE™

**OSPT Alliance**
- Vendor neutral, with no single supplier lock-in
- Fast, secure, easy fare payments, delivered cost-effectively and simply
- Management and evolution of an open, secure standard
- Open to all to transit and related ecosystems

**CIPURSE**
- Optimized for contactless and NFC (Near Field Communication)
- Disruptive, bottom up approach
- Multi-application support means flexibility for technology providers
- Certified and secure through rigorous testing and AES-128 security

Copyright © 2016 OSPT Alliance. All rights reserved.
OSPT Alliance HCE Working Group

Provide audiences with information about using mobile NFC technology to supplement traditional ticketing types and in other sectors

Engage transport stakeholders and other connected parties to understand requirements

Evolve CIPURSE Mobile to support current and future HCE technology

Copyright © 2016 OSPT Alliance. All rights reserved.
A brief introduction to HCE

HCE

- HCE is software emulation of a tamper resistant hardware device
- It simplifies traditional business models by eliminating the Secure Element (SE) owner
- Primarily used in retail payments, it can bring great benefits to transport ticketing too and beyond

A good fit for transit
HCE and transport ticketing – opportunities and challenges

Value to operators
• Cost effective
• Autonomous alternative
• Low investment
• Leverages existing infrastructure
• Enables interoperability between different closed loop systems

Constraints of ecosystem
• Proprietary incompatibilities
• Throughput
• Fragmented user base
• Network coverage
• Business rules
## Different ways to implement HCE

<table>
<thead>
<tr>
<th>Pure HCE</th>
<th>Hybrid HCE</th>
<th>Online HCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple but vulnerable to malware, regular key change vital</td>
<td>More secure but requires Mobile Network Operator (MNO) or other third party involvement</td>
<td>Cloud brings flexibility but also availability, latency and authentication issues</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Account based HCE</th>
<th>Offline HCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better customer service, but requires backend processing</td>
<td>Good fit for transit architectures, enabled by CIPURSE flexibility, requires tokenization</td>
</tr>
</tbody>
</table>
**Hybrid HCE**

Hybrid HCE combines HCE with using a SE to store keys and data

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Highly secure</td>
<td>• Requires ability to access SE from mobile app</td>
</tr>
<tr>
<td>• Tamper proof storage</td>
<td>• SE must be tailored to HCE application</td>
</tr>
<tr>
<td>• Protects from malware attacks</td>
<td>• Changes to infrastructure needed</td>
</tr>
<tr>
<td></td>
<td>• Involvement of SE owner, either MNO or OEM</td>
</tr>
</tbody>
</table>
Online HCE uses a remote SE stored in the cloud. The phone communicates with it using Application Protocol Data Unit (APDU) commands over a secure connection.

**Benefits**
- Existing infrastructure
- Independent
- Credential can’t be stolen
- Fewer vending machines
- Open API

**Challenges**
- Availability
- Latency
- Authentication
Account based HCE requires backend processing and turns the phone into a key for accessing services

Benefits

• More flexibility from wider variety of ticketing types
• Phone acts to supply identity only, with processing done on backend
• Impersonation, stealing and key re-use risks from HCE reduced as CIPURSE recognizes user ID as valid in real-time

Challenges

• Requires backend processing
• Greater opportunity for fraud
Offline HCE combines offline credentials, NFC phones and transport network infrastructures

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Good fit for asynchronous nature of transit systems</td>
<td>• May lack security but mitigations are available from existing system practices</td>
</tr>
<tr>
<td>• Can support multi-device approach including smart cards</td>
<td>• Today, tokens are not yet supported but work is underway</td>
</tr>
<tr>
<td>• Opens up the option of cross sector and cross operator collaboration</td>
<td></td>
</tr>
</tbody>
</table>
## A few words about tokenization

**Tokenization a good match for existing transit architectures**

- Transport products are already a form of token
- Additional protections like shadow account management often already in place
- Good preparation for interoperability

**Token Service Providers – who to choose?**

- Payment ecosystem TSMs come with constraints ill matched to transit needs
- Transit authorities must serve all, not just those with bank cards
- Ideally placed to create own services based on open standards

**Risk management and protecting tokens offline**

- Uses similar check and balance processing to existing transit model
- But software based tokens easier to attack than cards
- Tokens can be protected by obfuscation, use of TEE and other methods

---

Copyright © 2016 OSPT Alliance. All rights reserved.
A sample use case: the virtual ticket vending machine

CIPURSE uses the same standards software for all situations

Providing APIs to a mobile based vending app is a small step
Key benefits to using CIPURSE with HCE

Future proof way to implement → Brings added security benefits → Mitigate obvious weaknesses of HCE → Multiple options for implementation, to fit operator needs

Opens up possibilities for interoperability → Flexible and fits into existing ecosystem → Supports different types of implementation → But best approach may combine elements of several

Open standards mean no more vendor lock-in → CIPURSE standard free to download → Throughput and availability concerns alleviated → Network coverage no longer an issue with tokenization
Please join us in our future work on HCE

To review the impact of HCE on CIPURSE spec.

Outcome of this review may lead to developing:

- Faster, simpler authentication
- Asymmetric algorithms
- Elliptic curve
- Components specification
- CIPURSE Token Profile
- Implementation standardization
- Certification of HCE implementation
Introduction
What is HCE?
Implementing CIPURSE with HCE
Beyond transport ticketing
Conclusion and questions
CIPURSE and HCE will work beyond transport ticketing

- Mobile value added services
- Multi-applications
- Event ticketing
- Access control
- Loyalty
Introduction

What is HCE?

Implementing CIPURSE with HCE

Beyond transport ticketing

Conclusion and questions
Join the discussion

- There are many ways to get involved:
  - HCE Working Group
  - Systems-level Standardization Working Group
  - Technical Working Group
  - Certification Working Group
  - Mobile Working Group
  - Marketing Working Group

- Become a member and have your say…

The session is part of a series of webinars available from [www.osptalliance.org](http://www.osptalliance.org)
  - *Open Standards in Fare Collection: An Introduction to OSPT Alliance and CIPURSE*
  - *The Future of Transport Ticketing Systems: Technical Introduction to CIPURSE*
  - *CIPURSE Mobile: Supporting NFC Services Beyond Payment*