Horizon 2020 ETC 636126

Low cost implementation strategies

–

Deliverable D7.6

May31st 2016

Contents

1 Low cost implementation strategies

The deliverable is described in the Grant Agreement as "*The objective is to provide a low-cost solution for both existing terminals and new terminals to operate in the interoperable account based ticketing system. We will define low cost implementation strategies of the interoperable ID-layer both for existing and new infrastructures.*

For existing infrastructures, this means the integration of GST with reader software and fare media.

For new infrastructures we believe ABT (handling all complex products) in combination with only standard products on anonymous card centric systems, can lead to a significant reduction of infrastructure investment and maintenance, e.g. through the use of standard readers with all scheme specific software included in an intelligent SAM that is remotely upgradeable (Similar to the management of the SIM cards by Mobile Network Operators)."

This Deliverable is part of work package 7: "*Define and Develop Interoperable ID-layer*" and was produced while referring to the following specifications:

- GST V2.12
- STAS V1.24

Information contained in this report includes:

1. Questions that were researched based on key market trends (this section);
2. Resulting possible implementation strategies and supporting solutions in association with an ETC ABT project (second section);
3. A description of the sample reference implementations, built as part of the ETC demonstrator lab in Amersfoort/Netherlands, to assist potential ABT implementers (Section 3).

1.1. Goal of the low cost implementation strategies

The objective of the interoperable ID-layer is to provide the technical means to cost-effectively cross- accept fare media. To this end, the Generic Secure Token (GST, see Deliverable 7.4 for an example of an implementation and its specification), Secure Token Acceptance Sensor (STAS, see deliverable 7.1 Interface Specification Document) and ABT are defined by the ETC.

The ETC is also reporting on possible means to lower the cost of achieving the interoperable ID-layer's goal.

First, this encompasses direct costs associated with the procurement from the market of whatever hardware, software, and services may be required.

Secondly, this report is also encompassing other indirect costs such as related to the deployment phases involved with rolling out a ticketing system; as well as the cost implications of maintaining such a system and having to cope with all possible eventualities, including an unexpected and improbable breaking of its security.

Lastly but not least, although ETC ABT direct and indirect costs are the main target of this work, experience has shown that implementation costs are also made of other factors that are not necessarily under the control of the party responsible for implementing a given ticketing system.

Per instance, having to maintain side-by-side legacy fare-media with new ones.

In TfL[1]'s case, the implementation of an ABT solution leveraging EMV payment cards as transport credential was originally devised as a way to reduce the cost of fare-media issuance and related services; more than 8 years later, TfL is maintaining three systems side-by-side[2]:

1. EMV payment credential used in combination with TfL transport network ABT systems (launched in 2012);
2. ITSO (U.K. national standard specification for smart ticketing); and
3. Oyster (TfL 2003 electronic ticketing used for transport in Greater London).

Implications resulting from having to maintain several systems side-by-side are many, some are positive (e.g. convenience to users) other are negative (e.g. fare price increases due to a higher total cost of ownership).

At a time where mobile technologies are becoming so pervasive, we cannot put aside TfL's pioneer experimentation as an isolated case, even though it does remain an isolated experience to date. We must anticipate new modes of interaction between mobile users and transport ticketing systems, even future unknown ones, within manageable costs.

On one hand, the account-based concept can assist coping with future adaptations of a ticketing network, as it limits the functional role of the acceptance network.

On the other hand, ideally, ETC should provide means to address situations that are not directly related to its ABT solution, such as where other systems have to be maintained side-by-side (e.g. TfL having to maintain Oyster for passengers without payment cards, and ITSO for compliance with national standard specification).

Consequently, researching on low cost implementation strategies for a successful ETC ABT solution has required a product development approach which:

- Identified key trends from the market, suppliers, and developer ecosystems that are relevant to the ETC ABT solution.
- Provided non-prescriptive commodity-like solutions to adapt an ETC ABT implementation to the constraints and opportunities that potential implementers will inevitably be facing.

1.2. Ticketing requirements

Across this report, information reported was tested against several fundamental requirements. For readability reasons, fundamental requirements evaluations are not repeated across the document; they are listed here below:

- *Speed* (GST/STAS transaction below 500ms);
- *Security* (GST/STAS specification fully implemented; provide secondary means of protection);
- *Certification* (System components must pass a test against the GST/STAS specification; non-GST/STAS components can be specified using non-proprietary information);

[1] Transport-For-London / U.K.

[2] http://content.tfl.gov.uk/ppp-20140226-item04-future-ticketing.pdf

- *Ticketing scheme control* (e.g. ability to update the STAS, remotely, as it forms the point of acceptance in the network);
- *Cost* (e.g. resulting STAS compliant point of acceptance equipment cost must be less than conventional alternatives).

1.3. Opportunities

Besides the potential cost reductions opportunities created by the ETC ABT system approach, several areas of further potential cost reductions were identified.

These areas of opportunity were listed as part of brainstorming sessions involving representatives of the various tiers forming a transport-ticketing network, as well as those of payment networks. Eventually, the focus on transport ticketing was emphasized by taking in consideration the main factors related to a mobility scheme's total cost of ownership.

Based on the feedback collected during these sessions, cost factors are many, such as:

- Procurement costs (fare-media, reader, applications, SAMs, etc.…),
- Certification costs,
- Pilot testing costs (when implementation is not yet optimized/industrialized),
- Roll-out costs (once implementation is optimized),
- Remediation costs in the event of damaging security weakness, or failure,
- Capital assets maintenance costs,
- Operational costs (such as revenue collection costs),
- 'Not-on-us' interoperability costs ('Not-on-us' being fare-media from another security domain that is not compatible with GST/STAS specification).

The following paragraphs summarize selected relevant trends and the questions they put in relation to lowering the cost of implementing ETC ABT in your transport network.

1.3.1. Leveraging hardware and software trends

ETC ABT (with the usage of GST), combined with today's electronic hardware and software technology advances can be leveraged and enable radical engineering of new generations of point-of-acceptance.

A point-of-acceptance device can be designed as modular and retro-compatible with legacy operational environments and with payment networks. Indeed, after all, legacy smart ticketing and EMV technologies are 20 years old! Emulating such technologies side-by-side with ETC ABT is entirely doable. This was proven as part of this work by building a demonstrator described in Section 3.

Furthermore, Electronic components cost a fraction of what they used to cost 20 years ago.

Recent adoptions of NFC and EMV technologies by world leading mobile manufacturers have reinforced the industry ecosystem and created numerous electronic components offerings.

As a result, a terminal can be made standalone and autonomous through various types of communications (synchronous/asynchronous, mobile/Wi-Fi, …), for a fraction of the procurement and operational costs usually implied by conventional ticketing devices and transaction acquiring systems; considering that maintenance costs are usually a recurrent % of the procurement cost, total cost reductions can be very significant.

Question 1: What radical engineering technics can leverage ETC ABT to provide low cost implementation strategies?

- ⇨ Expand in section 2 on electronic engineering advances using:
  - Latest commercial SAM hardware as a trusted execution environment,
  - Front-end NFC and contactless front-end electronic components,
  - Latest processors,
  - Complete Android or Linux based mobile devices.

1.3.2. GST cost reduction

The ETC requires the fare-media to perform GST advanced cryptographic work, such as using Elliptic Curve, and therefore require advanced chip based technology. This chip technology has many advantages but comes at a price.

On the other hand, emulating GST within the secure area of a SAM and securely storing the resulting data, fully encrypted, onto a fare media opens up new possibilities; such as using a fare-media that does not have the advanced cryptographic capability required by GST.

Expert views suggest that advanced chip based card technology unit procurement cost is usually between 1 and 2 euros; while lower-end, but secured enough, card technology can be as low as 15 cts to 45 cts. Thus providing a potential procurement cost reduction ratio from **7 to 1 or even 13 to 1**!

Moreover, such intermediation of the GST processing by a SAM provides other advantages:

- Progressive issuance of GST fare-media in parallel with an existing population of legacy fare media;
- Including other fare-media than smart cards, such as NFC chip based or HCE. Therefore, being able to accept mobile applications issued by other entities, such as Banks or Merchants.
- Being able to develop and maintain a single ABT application that interoperate on multiple fare-media technologies.

In fact, the reference application built as part of the ETC ABT demonstrator for low cost implementation strategies performs GST functionality emulated by a SAM on a modular reader board that is pre-certified for contactless EMVCo L1 and NFC Forum, and is compatible with following protocols:

- ISO/IEC 14443 A & B,
- MiFARE™,
- ISO/IEC 15693,
- FeliCa™,
- ISO/NFC 18092,
- NFC-IP1 peer-to-peer.

Question 2: What implementation strategy can enable lower-end fare-media technologies without compromising ticketing requirements?

- ⇨ Expand in section 2 on using a SAM proxy implementation to implement GST/STAS mapping stored onto a lower-end fare-media without EC crypto capabilities,
- ⇨ Expand on using a card technology agnostic modular reader board to implement emulated GST for the broadest range of contactless technologies.

1.3.3. STAS cost reduction

In ETC ABT system specification, the STAS is essentially a pass through device. This greatly reduces the costs associated with establishing and operating a ticketing network.

On the other hand, implementing any additional software into a ticketing network points-of-acceptance usually involves third-party proprietary equipment of various configurations. As a result, implementing STAS may involve integrating functionality across several system components (Terminal Application, SAM software, Device Management System, Revenue Collection System, etc.) which may result in unwanted implementation costs; especially when considering that this third-party equipment may have to be maintained by different contractors and use different operating systems and capabilities.

In TfL's case, public figures about the cost of ownership of such systems are a clear indication that such experiment is not compatible with most transport authorities' budget:

66 million[3] pounds a year service cost for the maintenance and availability of ticketing and fare collection equipment,

65 million[4] pounds to adapt Transport for London's proprietary Oyster smart card technology to read cards meeting the open ITSO standards,

The acquiring and processing cost of accepting bankcards,

The cost of developing and maintaining TfL own systems (e.g. Transit Fare Calculation Engine, Settlement and reconciliations, etc.…).

ITSO SAMs (ISAM) procurement cost[5] is another indication of potential cost reduction as it concerns an isolated piece of hardware and software that appeared pivotal in most low cost implementation strategies.

ISAM procurement costs are anywhere between 70 (or 92€) and 105 pounds (or 138€). This is for the SAM for ITSO only (not including Oyster; not related to contactless payment card acceptance).

Expert views suggest that today's advanced SAMs procurement cost can be less than 15€ (such as the SAM used as part of the ETC demonstrator to provide STAS functionality, backward compatibility with existing smart cards and tickets, and forward compatibility with NFC mobile applications). Thus providing a potential procurement cost reduction ratio of **6 to 1** just for the smart card functionality!

Beyond the SAM itself, recent technology advances are also enabling elegant retrofitting of new capabilities into legacy terminal equipment.

In Section 2, we will present how we were able to implement ETC ABT solution side-by-side with an existing conventional smart cards & tickets solution by plugging into the legacy terminal a small electronic board with an advanced SAM, its own CPU, and a new generation front-end chip.

This provides an alternative to having to upgrade the existing legacy reader, terminal, and their applications, which often results in cost between 300€ and 2,000€; thus providing a potential procurement cost reduction ratio of **5 to 1 or even 40 to 1**!

[3] https://tfl.gov.uk/info-for/media/press-releases/2014/july/tfl-and-cubic-continue-partnership

[4] http://www.railwaygazette.com/news/passenger/single-view/view/oyster-begins-accepting-national-rail-itso-smart-cards.html

[5] https://www.itso.org.uk/about-us/itso-prices-2016-17/

Another relevant element of comparison concerns the case for an autonomous STAS terminal; such device is available within the ETC demonstrator and costed around 100 euros (refer to Section 3). In comparison, the procurement cost of a smart ticketing validator for bus is usually around 4,000€ [6]to 8,000€ per bus. Thus providing a potential procurement cost reduction ratio of **40 to 1 or even 80 to 1**!

Question 3: What implementation strategy can enable a lower point-of-acceptance equipment cost without compromising ticketing requirements?

- ⇨ Expand in section 2 on using a SAM centric STAS implementation to minimise the impact on 3rd party equipment,
- ⇨ Expand on using modular hardware to add-on STAS capability to a preferred hardware (e.g. adding EC cryptographic capability),
- ⇨ Expand on using autonomous STAS terminals to enable OS agnostic terminal applications on any vehicle.

1.3.4. End-user expectations

Today, the vast majority of ticketing systems are still either paper based or using smart cards and RFID tickets in conventional closed-loop systems.

Recently, transport networks have experimented with consumer technologies borrowed from the fields of commerce, such as Mobile Ticketing using bar codes, NFC Mobiles, or EMV Contactless Payment Cards used as transport credential.

This diversity of system is creating end-user habits that a transport stakeholder may be required to support as part of the ABT user experience.

As a result, a transport stakeholder tasked with the mission to implement a cost-effective cross-acceptable fare media faces additional challenges when aiming to achieve ABT cross-acceptance between legacy and emerging solutions, together with the GST/STAS ABT.

Possible desired implementations				
GST	**Conventional Smart Cards / Tickets**	**QR/Bar code**	**NFC Mobile**	**EMV**

In new infrastructures, requirements other than related to the ETC may imply that other implementations must reside side-by-side with GST and its ABT solution.

Per instance, an e-ticketing operator may be required to accept other fare-medium such as open-loop EMV credentials, local closed-loop stored value/tickets, or NFC mobile phones. This is often dealt with by replacing existing terminals, SAMs, and related applications. However, our work shows that recent technology advances enable multiple solutions, such as leveraging the SAM as an execution environment, to support multiple applications without requiring the terminal to perform intelligent functionalities; or such as adding a modular reader board capable to operate existing and new protocols.

[6] http://www.eurotransportmagazine.com/19165/news/industry-news/open-platforms-transport-saves-millions-bus-companies/

Question 4: What implementation strategies can enable both GST/ABT and other implementations to reside side-by-side without negatively affecting infrastructure' capital and/or operational costs?

- ⇨ Expand in section 2 on using a modular architecture to optimize implementation costs,
- ⇨ Expand on potential technical and commercial barriers to a proper integration of desired implementations together with ETC ABT.

1.3.5. Off-line transaction environements

A transport stakeholder may be faced with part of its transport network that will remain off-line for significant periods.

ETC solution was designed to cope with situations where the STAS is occasionally off-line. In a situation where a STAS will be off-line whenever interacting with a GST, the ticketing system will be operating in a degraded mode for this user.

Off-line operations may be dominant in your ticketing infrastructure, as conventional smart card system were designed to operate off-line and only required to report collected data to a remote central system on a batch mode (e.g. every 15 minutes, every day, every week).

In such situation, a proxy implementation of the ABT Account Management System can be deployed within a SAM; thus opening up new possibilities.

Question 5: What implementation strategy can enable off-line environments to become an integral part of the ETC ABT network?

- ⇨ Expand in section 2 on using a SAM centric implementation to serve as ABT Account Management System proxy (i.e. provide online authorisation off-line & safekeeping of relevant security keys and operations).

1.3.6. ETC ABT Backward compatibility

The ETC recognizes that green field situations are not the majority of ticketing system implementations. It is often economically or technically impractical to replace existing contactless smart cards (or other fare-medium) and points-of-acceptance at once.

Question 6: What implementation strategy can enable a cost effective integration of GST and its ABT solution, with existing contactless smart cards (or other fare-medium), and/or with existing ticketing point-of-acceptance equipment?

- ⇨ Expand in section 2 on using a SAM centric implementation as a backward compatibility solution.

1.3.7. ETC ABT Forward compatibility

Many transport stakeholders are required to prepare for future integration of systems that are either external to their ticketing network (e.g. EMV International Branded Payment Cards as transport credential) or not yet existing (e.g. new fare-media technology required in case an existing technology is hacked, as in 2008 MiFARE™ Classic [7]).

Providing an ABT offers several opportunities compared with disconnected systems. Moreover, preparing the STAS to be remotely upgradeable and ready to accept new applications and fare media technologies increases potential forward compatibilities.

Question 7: What implementation strategy can enable a cost effective readiness to accept other fare-media than presently assumed?

- ⇨ Expand in section 2 on using a modular reader board with maximum compliance with open standards such as defined by the ISO or NFC Forum, and multiple SAM slots.
- ⇨ Expand on using a SAM-centric EMV credential acceptance.

1.3.8. ETC ABT flexible roll-out

In many situations, such as often found with bus operations using rented vehicles, small capacity vehicles, car-pooling schemes, or during a pilot project phase, and autonomous device requiring no particular installation is desired.

Question 8: What implementation strategy can enable flexible implementations of an ETC ABT network?

- ⇨ Expand in section 2 on using a low cost Android Devices with an integrated SAM centric implementation.

[7] Flavio D. Garcia, Gerhard Koning Gans, Ruben Muijrers, Peter Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling mifare classic. In Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, ESORICS '08, pages 97–114, Berlin, Heidelberg, 2008. Springer-Verlag.

2. Low cost implementation strategies

2.1. Solutions

2.1.1. Role of the mobility service operator

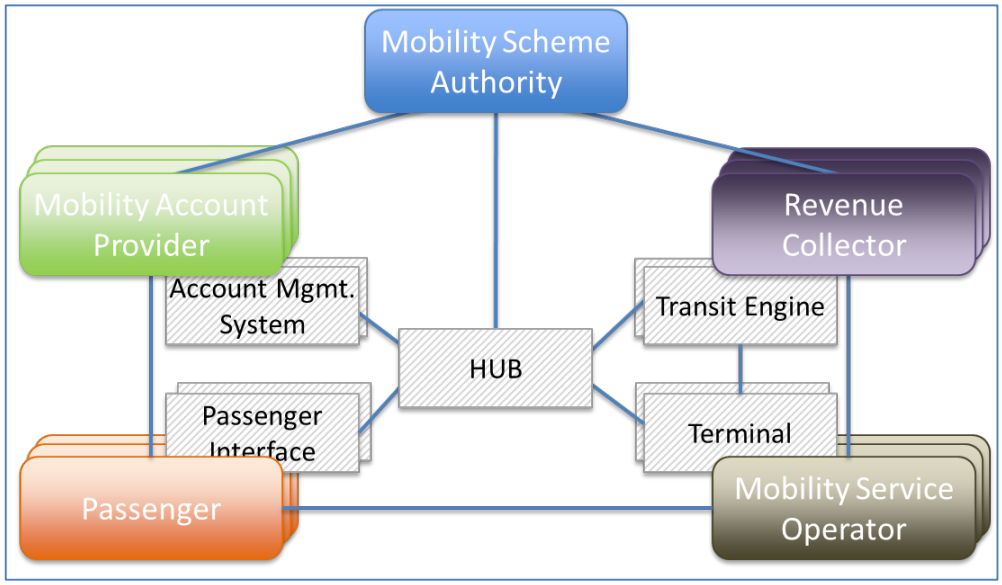


Figure 1: ETC ABT four corners model

In ETC ABT's four corners model, Terminals located at the points of contact of passengers with the transport network serviced by the Mobility Service Operator form the points of acceptance into the Mobility Scheme. They are:

- The Points of Acceptance (POA) for the Passenger to avail for the mobility services (i.e. the creation of the mobility service contract for the desired trip);
- The POA of whatever fare-media Passengers can use (GST/STAS compliant and others);
- The POA between the fare-media and the Transit Engine of the Revenue Collector;
- The POA between the fare-media and the Hub linking it to both:
  - The Passenger Interface (e.g. its travel history on mobile phone), and
  - The Mobility Account Provider's Account Management System (e.g. a Rail corporate travel pass).

In an international branded payment card network, terminals are usually provided by the Payment Acquirer (the card network four corners model's equivalent of the Revenue Collector). In a transport network, a particular challenge comes from the fact that terminals are usually provided by the Mobility Service Operator, while the acquiring responsibility is often with the Revenue Collector.

In a transport network that intends to take advantage of the ABT solution, other solutions provided by the Mobility Service Operator (e.g. conventional smart card/tickets, and/or NFC mobile applications, and/or payment cards networks using EMV) are to be accommodated for.

As a result, the POA is often composed of several terminals integrated together through limited underlying common layers (e.g. contactless and NFC radio layer, and application selection layer). The consequences are very significant as the number of terminals built into a POA drives not only the initial procurement cost and integration complexity but also the recurrent cost of maintenance and operations.

However, our work shows that it is possible to displace the Terminal's functions that are related to both the Revenue Collector and the Hub, by abstracting the relevant data and processing layers forming them. With such a solution, it becomes possible to implement these abstracted layers into small and modular form factors commonly called 'secure elements' (e.g. SIM cards, embedded SE, SD cards, SAM).

This way, the secure element can be provided and managed by the entity responsible for revenue collection while the Terminal can remain provided and managed by the entity responsible for delivering the mobility services.

Moreover, the displacement of relevant terminal functions into a small and modular form factor can **enable major cost reductions**.

It also creates new possibilities in terms of acquiring transactions of different protocols than the ETC ABT prescribed protocols; thus **opening up further cost reduction** should integration with existing and future protocols be required.

Finally, this advance in POA technology can also enable the acceptance of other applications than those initially prescribed by the ABT and existing services of the Mobility Service Operator. Per instance, a Mobility Service Operator may require in the near future that a Mobile Application interacts with its Terminals (e.g. to manage a rail station Ticket Vending Machine). **Advance in POA technology can enable new forms of multi-application 'platform'** wherein applications do no need to co-reside on a same secure element held by the user; instead, the POA technology is leveraged to accept multiple applications, by remotely managing the POA 'secure element'. The reconciliation between resulting system interactions (e.g. the transactions resulting from the interaction between the user and the POA) is then performed essentially by the routing role of the Hub and the Revenue Management role of the Revenue Collector; the Terminals does not need to be intelligent.

In essence, the small modular form factor acts an execution environment for multiple application networks (e.g. transport closed-loop, transport ABT, open-loop payment, closed-loop mobile application) and potentially reduce the total cost of ownership of both the Mobility Service Operator and its partners. From this perspective, the Revenue Collector can act as a cost effective 'Acquirer' of not-on-us Applications.

2.1.2. Advances in technology

In parallel with the evolution of Mobility Schemes triggered by the transformation of both mobile phone and payment networks, electronic components have greatly evolved.

Today, an electronic chip, such as used by a secure element, embeds more processing power than a personal computer used during the early days of smart cards.

The management of such secure element (e.g. provisioning of the data, remote upgradeability in the field) is strong of 20 years of experiences across sectors (e.g. payment, transport, telecommunications). These techniques (e.g. key management, scripting and messaging) are supported by a large population of professionals across the globe.

Besides the secure element, the massive production of consumer mobile devices, such as mobile phones and tablets has resulted in very affordable electronic components that have far more capabilities than most electronic components that are still in use in existing payment and transport terminals. Thus opening up many opportunities to re-invent the bill of material of a POA used in transport networks.

These facts have led us to propose a Solution Architecture which:

- Leverages the secure element as an execution environment;
- Decreases the role of the terminal to minimal functions, with minimal trust; thus achieving a more secure environment;
- Leverages mobile NFC electronic components to bridge mobile and contactless communications to the Mobility Scheme's transaction acquiring functions;
- Uses widely available mobile hardware (e.g. android tablets) as the basis for an autonomous POA device.

We consider this exercise as especially motivating as results have surpassed our highest expectations, both in terms of effectiveness and in terms of cost. The following paragraphs are detailing some of the key aspects of the resulting Solution Architecture.

2.1.3. SAM centric architectures

2.1.3.1. The case for SAM

In the following paragraphs, the solution architecture centred on a Secure Application Module is first justified; then it is described in more details.

The first justification concerns the choice of the secure element's form factor.

Indeed, some of the most successful OEM mobile consumer products are using secure elements of different form factors than a SAM; per instance, an embedded secure element which is welded onto the mobile main printed circuit board; or part of the front-end NFC electronic component; or a Telecommunication SIM card.

Recent choices made by OEM mobile manufacturers serve their own business strategies; which might include a desire to either further reduce the mobile phone's bill of material or increase the manufacturer's independence. Per instance, Apple iPhones are known to use a secure element that is an integral part of the NFC front-end electronic component; while Samsung Galaxy phones are known to use an embedded secure element.

However, such form factors also come with a major drawback: What if the secure element fails due to hardware failure or security attacks? What if the secure element supported hardware cryptography is not powerful enough few years from now?

Today, OEM Mobile devices are not designed for a lifetime that compares with transport network infrastructures. A mobile phone lifetime is in terms of few years while the reality of transport network infrastructures suggests that their lifetime is in terms of a decade or more. **Wherein the decision to use a SAM swappable form factor for ETC ABT**.

2.1.3.2. Re-inventing the role of the SAM

Many SAMs in the market perform authentication, verify and generate signatures: they may also manage a secure channel and usually return plain data to the validator. Even though these SAMs perform complex tasks, the solution remains Terminal centric, considering that the validator is responsible to perform the transaction and to update the card. The role of the SAM is thus limited.

On the other hand, recent advances in technology have resulted in so much additional processing capability that a SAM that is based on latest chip technology, can perform some of the processing commonly performed by the Terminal. Moreover, such a SAM can perform cryptographic processing in nanoseconds while most terminal CPUs perform the same processing in milliseconds.

In an increased scope of processing, the SAM would need to expose its functionality to the application driving it (such as from the Terminal; or directly from a user Card should a direct communication path be available between the Card and the SAM). Besides, the SAM would also need to embed the information required to interpret the data of the application driving it.

2.1.3.3. Card technology agnostic SAMs

Assuming that points made in 2.1.3.2 are supported, additional processing related to the interpretation of the communication protocol used by the card technology driving the application could also be included in the scope of the SAM.

In such a scenario, instead of establishing a secure channel between the card and a Terminal through a session key generated by the SAM, we could imagine all processing performed in clear to remain within the SAM execution environment, without ever releasing any security key outside of the SAM.

This would in effect be using the user Card as a secure storage of data that only a SAM can interpret. In order to avoid cloning of the Card data, the Card Technology would need to support:

- A unique card serial number,
- A secure authentication method,
- Read/write plain or cipher,
- A unidirectional counter,
- Secure update verification (optional).

2.1.3.4. Card application proxy functionality

In order to interpret the data from the card, the SAM needs to own a mapping of the data expected from the user Card versus whatever rules the application expects to be performed upon predefined conditions.

This would enable the creation of an image of the Card data within the SAM's execution environment, thus the term 'Card application proxy'. With the proper basic functionality built into the SAM, the management of the Card application would no longer require a modification of the Cards and Terminal data or software, but only require new versions of the mapping.

For this solution to be flexible enough, the management of data definitions (directories, files, …) would need to be part of the SAM basic functionality too; thus providing ways to create new applications in the field simply by sending the right updates to the SAM (with the right access conditions).

In a Card application proxy mode, one would read all data files related to an application from the user card and send them to the SAM. The SAM would then validate each file by verifying a signature. The SAM would create a temporary representation of the card files in the SAM RAM memory with the behaviour defined by a mapping for this application. The mapping would provide the tags applicable to each field, defining the address, the size in bits and the behaviour of data. This would enable the SAM to autonomously perform processing on each field using the rules and constraints expressed by the relevant tags.

In the advanced SAM used by ETC ABT demonstrator, an example of such a Card Application proxy is able to make use of around 40 different data tags with different behaviours, such as: counters, balances, card transaction counters, load transaction counters, transaction types. Each tag has its own rules and update constraints.

Finally, when all the Card data inside the SAM is processed, the SAM can encrypt the result and return an indication to the driving application that it is ready to write back to the Card, using a single simple APDU.

2.1.3.5. Integrating a transport application into a SAM centric architecture

Besides acting as a Card application proxy, an advanced SAM can also maintain data related to its communication with a host, thus providing a form of integrity for asynchronous messaging communications that are used by most transport ticketing system infrastructures.

The SAM signs data intended for the host, using logs and answers, verifies signed data from the host, and perform cryptographic work.

The same SAM can also be used as the counter-part system node on the remote host; in effect, the SAM fulfils the role normally fulfilled by an HSM. It generates cryptograms for transactions, generates signatures and verifies data exchanged between the host and the terminals.

This would provide numerous advantages, such as:

- A single set of commands (APDUs) and standard operations for both the Terminal SAM, the host, and the application;
- A low cost execution environment that can be used with any personal computer and ISO7816 compliant reader;
- Higher flexibility;
- High security (no key is ever released outside of the SAM);
- Support for multiple issuers, multiple system tiers;
- Interoperability with multiple card Technologies;
- Field upgradability through asynchronous messaging.

2.1.3.6. Unknown facts uncovered:

- Effectiveness of the solution: The Advanced SAM used for the demonstrator performed well below the expected transaction time.
- Cost of the solution: The sample used for the demonstrator public list price is below 20€.

2.1.4. SAM centric terminal components

2.1.4.1. The case for inventing a SAM centric terminal component

The ABT solution removes the need for complex Terminals by displacing most processing to the back-end. Consequently, we have researched on a cost optimized terminal component; wherein Mobility Services related functions would be specified for and provided by the Terminal; while the Revenue Collection services would be specified for and provided by the SAM and the electronic components of a printed circuit board supporting the SAM.

While researching on this matter, we discovered that not only such solution is possible but also that such terminal component is:

- Already available and very cost effective (30€ to 50€),
- Used in several countries where it was devised as a mean to protect terminals from certain security attacks (e.g. back doors),
- Capable of handling a major part of conventional smart card and ticket processing (pending that a SAM centric implementation is used).

Contactless and NFC communications, security protocols, applications and data being abstracted within the SAM centric architecture, the terminal scope can be greatly reduced.

In a conventional architecture, a dedicated reader board part is used to handle contactless communications and another part is used to handle interfacing between all hardware components and to perform computing tasks.

In a SAM centric terminal architecture, the SAM can be chained to the fare-media by a series of components performing transparent processing. By 'transparent processing' we mean a specific task that the terminal has no access to, or no understanding of the data being processed. From an information security architecture's viewpoint, this means that only the physically tamper proof components (the SAM and the Smart Card) of the end-to-end processing chain are able to interpret the data.

These physically tamper proof components are also used to redirect processing to secondary components. In this architecture, the Terminal is a secondary component.

With such a concept, the primary components of the proposed architecture are:

- The secure element held by the user (e.g. a Smart Card),
- The advanced SAM,
- The Issuer HSM ('Mobility Account Provider' in ETC ABT model).

In order to build a demonstrator of this architecture, we needed:

- An electronic component that supports contactless communications (such as ISO 14443 based) and NFC communications directly, such as SWP based;
- A SAM technology that integrates the same (i.e. ISO 14443, NFC, and SWP interfacing)

We found an example of such electronic component and used it in various use cases. Some are described in the Section 3 of this document.

2.1.4.2. Unknown facts uncovered:

- Effectiveness of the solution: The SAM Centric Terminal Component used for the demonstrator performed well below the expected transaction time. It is available in several forms: as pluggable retrofit module, as desktop reader pad attached to a main processing unit, and as stand-alone android-based terminal.
- Cost of the solution: The Terminal Component sample used for the demonstrator public list price is below 40€. The stand-alone android based terminal public list price is in the range of 100€-150€.

2.2. Implementation strategies

Following is a comparison of various alternatives to reduce costs when considering ABT and possible desired implementations.

Desired Implementations	GST				Conventional Smart Cards/Tickets		NFC Mobile Applications	EMV		QR / Bar Code
Alternatives	(a) Backward Compatible	(b) Off-line	(b) Forward Compatible	(c) Greenfield	(d) Backward Compatible	(e) Forward Compatible	(f)	(g) Private Label	(h) Branded Networks	(i)
(1) Encode in existing terminal software	*	**	***	****	*****	******	*******	********	*********	**********
(2) Insert an Advanced SAM	*	*	*	*	*	*	**[1]	***[1]	****	*****
(3) Connect a SAM Centric Terminal Component	*	*	*	*	*	*	*	*	**[2]	***
(4) Use a SAM Centric Autonomous Device	*	*	*	*	*	*	*	*	**[2]	*

(*) Signification: Each additional asterisk suggests that the said alternative probably implies additional software or hardware to support the desired implementation. The more asterisks, the higher are implementation costs likely to be.

([1]): Without and advanced front-end NFC chip (such as embedded in alternatives 3 and 4), additional terminal software is required.

([2]): Branded payment networks EMV compliance enforces requirements, such as EMVCo certifications, that may not be possible unless an existing certified terminal centric EMV device is used.

.

2.2.1. Encode in existing terminal software

Pre-conditions:

- Existing terminals must be capable of complying with STAS transaction acquiring and receipt verification.

Impacts:

- Adapt the terminal to comply with STAS configuration and functions (STAS specification V1.24).
- Adapt the terminal to comply with GST (GST specification V2.12).

Purposes:

To provide ETC ABT STAS functionality to existing terminals, and support desired implementations side-by-side with ETC ABT solution.

Each desired implementation ((a) to (i)) has its own impacts, depending on the existing terminal configuration and provider conditions.

2.2.2. Insert an Advanced SAM

Pre-conditions:

- Available SAM slot on the existing terminals and ISO7816-3 compliant interactions with the SAM.
- The terminal SAM slots must also support always on, parallel processing, of multiple SAM slots.

Impacts:

- Adapt the terminal software to redirect processing to the Advanced SAM.
- Each existing terminal technology may require its own version of the software adaptation.
- In order to support other applications (other than ETC ABT) such as from NFC Mobile Applications (e.g. A Bank's mobile application), additional software impacts are likely.
- Advanced SAM can handle EMV processing but will likely require the communication and application selection abstraction layers to be implemented by the existing terminal software.

Purposes:

To provide ETC ABT STAS functionality to existing terminals (desired implementation (a)).

To emulate GST functionality with non-GST smart cards using the Card Application proxy functionality of the Advanced SAM (desired implementation (a)).

- Provide a backward compatibility with existing smart cards that may not support GST advanced functionality (e.g. Elliptic Curve cryptography).
- Provide an option to use low-end/cost smart cards with sufficient security (see 2.1.3.3) such as earlier versions of MiFARE™ DESFire or latest CIPURSE™ L or S profiles.

To support ETC ABT STAS off-line, and to perform Mobility Account Provider's Account Management System authorisation (desired implementation (b)).

To provide ETC ABT STAS functionality to greenfield deployment using third party terminals with an available SAM slot (desired implementation (c)).

To provide support for conventional Smart Cards/Tickets

- Backward Compatible: per instance, a MiFARE™ classic card data layout and processing rules can be implemented within the Card Application proxy; side-by-side with the ETC ABT implementation (desired implementation (d)).
- Forward Compatible: per instance, future addition to the Mobility Scheme of an off-line closed-loop access control application for transport personnel to access restricted area (desired implementation (e)).

To provide support for NFC Mobile Applications

- Accepting NFC Mobile Applications interactions and completing their processing using a SAM centric implementation is possible side-by-side with the ETC ABT implementation (desired implementation (f));
- However, some of the processing (e.g. near field communication and application selection) will likely need to be implemented by software within the existing terminals.

To provide support for EMV

- Accepting EMV private label interactions and completing their processing using a SAM centric implementation is possible side-by-side with the ETC ABT implementation (desired implementation (g) and (h));
- However, some of the processing (e.g. EMV contactless communication and application selection) will likely need to be implemented by software within the existing terminals.

Bar code implementation requires supplemental dedicated equipment and processing

2.2.3. Connect a SAM Centric Terminal Component

Pre-conditions:

- Available PC/SC-CCID, or CDC connection port (SPI connection port is also possible but was not available on the device tested.

Impacts:

- Either use the SAM Centric Terminal Component with its optional external antenna (e.g. to retrofit into an existing equipment without contactless or NFC capabilities, or with outdated implementation).
- Alternatively, use the SAM Centric Terminal Component with existing equipment's antenna.

- Depending on whether existing applications are implemented in the Advanced SAM, side-by-side with the ETC ABT, or are still present as a separate implementation within existing equipment; minor software adaptation of the existing terminal may be required to redirect the data to the relevant system tier.

Purposes:

Identical to 2.2.2 but with no, or less, impact on an existing terminal.

This alternative also works for terminal without available SAM slot.

In case NFC Mobile Application implementation (f) or EMV private label implementation are desired (h), all processing (e.g. including near field communication, contactless communication, and application selection, are built into the device).

Bar code implementation requires supplemental dedicated equipment and processing.

2.2.4. Use a SAM Centric Autonomous Device

Pre-conditions:

- None.

Impacts:

- None.

Purposes:

Identical to 2.2.3.

This alternative is also compatible for QR/bar code implementations (desired implementation (i)), using the device front camera (available in multiple configurations) and Android environment

3. ETC Low-cost Implementation Demonstrator

In order to assist transport stakeholders who are considering ABT implementations and require low-cost strategies, a functional demonstration was deployed as part of the ETC lab in Amersfoort/Netherlands. Following is a description of the demonstrator and how it supports some of the key low-cost strategies.

3.1. GST/STAS SAM Centric architecture implementation

The sample GST card used by the ETC demonstrator was used to test a SAM Centric implementation of the STAS using the SAM Centric Terminal Component (see 3.5.1).

3.2. GST/STAS Backward compatibility

Backward compatibility of a GST/STAS implementation with an existing smart card technology that is not capable of performing GST functionality (e.g. EC cryptography - MiFARE™ and CIPURSE™) was achieved with the SAM Centric Terminal Component and an Advanced SAM that is used as a GST proxy (see 3.5.1).

The Advanced SAM is using a symmetric key from the Mobility Account Provider to perform the Account Management System's online authorisation of the card/ticket presented at the point of acceptance.

All data stored onto the existing smart card/ticket are fully encrypted, except when it is processed with the RAM of the Advanced SAM.

Another backward compatibility scenario is when the same SAM Centric Terminal Component is used to process both GST fare-media and existing smart card or tickets that support a data layout and set of ticketing keys that are not related to ETC ABT, i.e. a 'legacy ticketing application'. This is possible and effective by:

1. inserting the SAM of the 'legacy ticketing application' to one of the 3 available SAM slots of the SAM Centric Terminal Component; and with few minor modification of the terminal software of the 'legacy ticketing application'; or
2. by encoding into the same ETC ABT SAM the mapping of the 'legacy ticketing application' data layout and ticketing keys.

In our tests, a conventional smart card applications mapping into the ETC ABT Advanced SAM took two weeks of design and build work. The duration of the test work depends on the test plans specified by the 'legacy ticketing application'.

3.3. GST/STAS Green field

An Android Autonomous Device that embeds the SAM Centric Terminal Component was used to process GST using the same Advanced SAM as in 3.2 (see 3.5.4).

3.4. GST/STAS Froward compatibility

The SAM Centric Terminal Component (see 3.5.1) is technically able to perform processing both for EMV contactless protocol and NFC Mobile Applications interactions.

Note however, that today's EMVCo certification process requires each particular EMV implementations, including its Acquiring domain, to be certified separately. EMV certification was not included as part of the demonstrator.

3.5. Equipment used in ETC demonstrator lab

3.5.1. SAM centric terminal component

This component is usable in a multitude of situations. In our case, we used it in combination with an advanced SAM to decouple the secure part of transactions between the SAM and the user card and perform terminal operations.

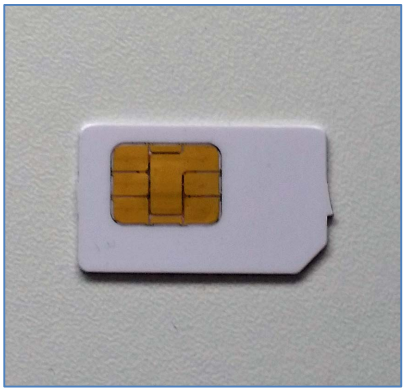
It provides ISO compliant slots for 4 SAM modules and directly access contactless cards through its embedded contactless front-end module. It also provides a direct channel from the SAM environment to the contactless card, thus allowing the SAM application to control the device in use.

Interestingly, beyond the direct SAM to contactless application, the device can be plugged into and computing device, such as an existing terminal, a stand-alone personal computer or EFT POS, or a host server, and can be used to act as a front-end device, a development environment, or a back-end device (such as a small SAM bank).

3.5.1.1. Specification:

- Power: 5V
- Dimensions: 71 x 39 x 8 mm
- Interfaces: USB 2.0; Serial TTL
- Protocols: PC/SC – CCID; CDC; CDC ACM (for Android connection); MSD (mass storage device)
- ARM 32bit CPU; Up to 4MB data flash
- Supports up to 4 SAMs; ISO clock up to 24MHz; TA1 up to f/8
- Performs direct transactions to contactless cards using SWP (1.7Mbps)
- Remote secure firmware update
- Complete NFC Interface; ISO 14443; ISO 18092; ISO 15693; Card emulation support
- External antenna accessory: Adhesive flexible antenna or PCB antenna

3.5.2. Advanced SAM



The advanced SAM used in the demonstrator proved extremely versatile. It was used well beyond the functionality normally expected from a SAM. This was possible mainly because of the sheer power of the chip used by the SAM but also because of the specific operating system functionalities. This operating system enables SAM centric and card technology agnostic processing. It embeds several abstracted interface layers: contactless and NFC communications, security protocols, and applications.

It operates using ISO APDUs and offers multiple commands required for all sorts of application, including public transportation and payment. Its meta-data handling engine allows a single application to operate simultaneously on several different card technologies by decoupling both the data and application function from the card technology; thus providing significant simplifications compared with conventional software approaches.

3.5.2.1. Specification:

- Interfaces: ISO7816-3 T=0 or T=1 ; SWP supports CIPURSE™ & MiFARE™ compatible protocols
- Communication speed: up to 1.25Mb/s
- Form factors: ISO7812 or 2FF / 3FF
- 3V / 5V
- 400kB of user memory
- CMAC / other diversifications

- Based on solid flash 32bit security controller
- Certified Crypto libraries: SHA-1 / SHA-224 / SHA-256; RSA up to 4096 bits (by hardware); 3DES, DES (by hardware); AES128/256 (by hardware); Elliptic curve cryptography (ECC) – 521bits
- Performance of the Asymmetric Crypto Processor for RSA and ECC calculations: 1024-bit Key Generation < 1s – 1024-bit Sign (full exp) < 60ms;„ Symmetric Crypto Processor for AES, (3)DES calculations: „ 256-bit AES < 10µs „
- Certification „ CC EAL 5+ High &„ EMVCo Approval
- True Random Number Generator
- 31 symmetric keys per directory, 1 Asymmetric key per directory

3.5.3. SAM centric pad terminal

This device is a contactless smart card reader/writer supporting any card of ISO 14443 A/B/F, and NFC. It includes a SAM slot for SAM centric architecture and is designed to be added to existing desktop equipment such as a POS or access control devices (either through USB or through an optional serial cable).

3.5.3.1. Specification:

- Power: 5Vdc / 0.3Amax
- Dimensions: 60.0 x 105.0 x 9.0mm
- Interfaces: USB 2.0; Serial RS232 or TTL; Wiegand and aBA (optional)
- Card types: ISO 14443A/B, Felica™, MiFARE™, Jewel™
- Driver: CCID
- Protocol: PC/SC
- Operating temperature: 0 to70°C
- Remote secure firmware update
- 1 SAM slot for ISO7816
- Optional kit for Evolis Dualys or Peeble printers

3.5.4. Android autonomous device

The Android autonomous device is a dual-processor device with a dedicated hardware for secure operations. With its capacitive touch 7-inch screen, it joins the programming flexibility of Android with the security of a dedicated hardware that can be used to perform operations with other NFC devices and contactless smart cards using a SAM centric architecture.

Its main characteristics are provided by a quad core processor, 1GB of RAM memory, 16GB of internal flash storage and an internal interface for 3G and 4G modems.

The secure hardware component part supports 4 SAM modules, contactless interface and antenna for ISO14443 and ISO15693, in other words, the main card technologies in use.

This device can be also connected to an accessory that provide permanent power supply, two open-drain outputs and four insulated inputs.

3.5.4.1. Specification:

- Power: 5,3V
- Dimensions: 312 x 158 x 30 mm;
- Interfaces:
    - USB host; Serial RS232; Wi-Fi - IEEE 802.11 b/g/n; Bluetooth 4.0
    - Complete NFC interface; ISO14443A, B, F; ISO18092; JISx 6319-4; ISO15693
    - SAM SLOTS: 4 SAM SLOTS; speed up to 1.25Mb/s; SWP enabled
- Operating temperature: 0 to 70°C
- Additional Characteristics: Quad core 1GHz processor; 1 GB of RAM; 16GB of flash storage SD card slot (up to 32GB); Moving sensor (3 axis accelerometer); VGA front camera
- Certifications: ANATEL, RoHS, IP-41 (for Android part)
- Vertical and horizontal installation
- Secure firmware update

4. Annex

4.1. List of Acronyms and Terms

Name	Meaning
ABT	Account Based Ticketing
APDU	Application Protocol Data Unit
CDC	Connected Device Configuration
CPU	Central Processing Unit
EC	Elliptic Curve
EFT POS	Electronic Funds Transfer at Point of Sale
EMV	Europay, Mastercard, Visa
ETC	European Travellers Club
GST	Generic Secure Token
HSM	Hardware Secure Module
ISAM	ITSO SAM
ISO	International Organization for Standardization
ITSO	UK National Standard IT Specification for Smart Ticketing
NFC	Near Field Communication
OEM	Original Equipment Manufacturer
POA	Point of Acceptance
QR Code	Quick Response Code
RAM	Random Access Memory
RFID	Radio frequency Identification
SAM	Secure Application Module
SD Card	Secure Digital Card
SE	Secure Element
SIM	Subscriber Identity Module
SPI	Serial Peripheral Interface
STAS	Secure Token Acceptance Sensor
SWP	Single Wire Protocol
TfL	Transport-for-London