EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system
work better for society.

Light Impact Assessment

TAP Revision 2019/20 – Closure of Open Point Chapter 4.2.10 related to Public Key Infrastructure

Contents

1. Context and problem definition

<table>
<tr><td>1.1. Problem and problem drivers</td><td>Ticket control equipment needs to read and check a barcode, it does so by using the carrier's public key, stemming from a public-key-pair generated by the carrier. Public keys can be freely distributed using IT industry standards. E.g. currently a number of keys are distributed via UIC website (via the UIC PUBLIC KEY MANAGEMENT WEBSITE") (https://railpublickey.uic.org)

Problem/need to be addressed:

The user of such public keys have to trust, that the keys origin from the right carrier and that they did not origin from a fraud carrier (e.g. result of a man in the middle attack). There is a lack of security layer ensuring authenticity of keys and owners.

The proposed standard for the handling of security elements (CEN/TS 16406) mandates a Public key infrastructure however the architecture of such PKI is not yet specified in detail.</td></tr>
<tr><td>1.2. Main assumptions</td><td>1. We received basic input information for the LIA from selected experts, which were recommended by the European Stakeholder Organisations. These experts work within national or international organisations – however we assume that they expressed the view of the European Stakeholder Organisation, which recommended them as contact point.
2. The role of specific specific entities mentioned in this LIA like the TAP KEY REGISTRATION AUTHORITY (see option 1 and 2) can be performed by existing organisations like UIC who already execute a similar function.</td></tr>
<tr><td>1.3. Stakeholders affected</td><td>
<table>
<tr><th>Category of stakeholder</th><th>Importance of the problem (*)</th></tr>
<tr><td>Railway Undertakings
(as distributor of public keys for their services)</td><td>4
There is a risk that a fraud carrier could distribute keys pretending that he is a specific (real existing) carrier. In this case the fraud carrier would steal revenues from ticket sales from the real existing carrier</td></tr>
<tr><td>Ticket Vendor
(as user/receiver from public keys to issue a ticket)</td><td>4
There is a risk that a ticket vendor might issue a ticket from a fraud carrier</td></tr>
<tr><td>Railway Undertaking
(as user/receiver of the public keys for ticket control)</td><td>4
The railway undertaking is not able to identify fraud tickets with his ticket control devices. As a consequence he would loose revenues.</td></tr>
</table>
</td></tr>
</table>

		Citizen (as user of rail transport buying a ticket) — 4: The customer might buy a fraud ticket without knowing that this ticket is a fraud ticket.
		Note: Other stakeholder than those mentioned above (e.g. vehicle suppliers, vehicle leasing companies or infrastructure managers) are not concerned by the problem
		**) 1=low; 5=high*
1.4.	**Evidence and magnitude of the problem**	The evidence of the problem was confirmed within bilateral meetings with stakeholders (e.g. UIP/VDV e-ticket, UIC) However the risk of fraud was not quantified/monetized by the stakeholders. The costs of the current public key infrastructure are very low considering that a railway undertaking changes its public key every 1-2 years and the costs of creating such public key are very low (<<100EUR)
1.5.	**Baseline scenario**	The current Open Point (chapter 4.2.10) will not be closed in TAP TSI.
1.6.	**Subsidiarity and proportionality**	Delegated Decision 1474/2017 Art. 14 (6) mandates the Agency to revise TAP TSI with the objective to facilitate the emergence of through-ticketing, integrated ticketing and multi-modal travel information and reservation systems.

2. Objectives

2.1.	Strategic and specific objectives	Strategic objective(s) of the Agency with which this initiative is coherent. ☐ Europe becoming the world leader in railway safety ☐ Promoting rail transport to enhance its market share ☐ Improving the efficiency and coherence of the railway legal framework ☐ Optimizing the Agency's capabilities ☐ Transparency, monitoring and evaluation ☒ Improve economic efficiency and societal benefits in railways ☐ Fostering the Agency's reputation in the world The specific objectives are: *A. To keep the risks of frauds in the framework of distribution of tickets and ticket control to an acceptable level.* *B. To design a cost efficient public key infrastructure suitable for existing fulfilment means (e-ticket, print-at-home, mobile phone ticket) however open for new fulfillment means such as chipcards*
2.2.	**Link with Railway Indicators**	N/A

3. Options

3.1. List of options	Baseline Option 1 – Distribution of Public Keys only via TAP KEY REGISTRATION AUTHORITY Option 2 – Distribution of Security Certificates only via TAP KEY REGISTRATION AUTHORITY
3.2. Description of options	**Baseline** The Open Point is not closed, Public Keys are distributed via different ways: e.g. a RU issues security certificates by itself and distributes them to other RUs. Or a RU distributes its keys via UIC or other organisations. **Option 1** Public Keys are only distributed via a TAP KEY REGISTRATION AUTHORITY. This authority checks the authenzity of the railway undertaking (does it exist, trusted contact persons in the organization) before it distributes the keys. The TAP KEY REGISTRATION AUTHORITY will revocate keys as well when necessary (e.g. key has been stolen). (TAP TSI would specify mandatory requirements applying to the TAP KEY REGISTRATION AUTHORITY) **Option 2** like Option 1 but The TAP KEY REGISTRATION AUTHORITY would issue security certificates (including the public keys). The TAP KEY REGISTRATION AUTHORITY will revocate certificates as well when necessary. The TAP KEY REGISTRATION AUTHORITY would be the only entity having access to an IT center which creates the certificate including the key. This infrastructure would allow the distribution of security certificates in high quantities which would be required in the context of future fulfilment methods like chipcard. This option is already implemented in DE in the framework of local public transport tariff and transport associations. (TAP TSI would specify mandatory requirements applying to the TAP KEY REGISTRATION AUTHORITY and the IT center producing the certificates)
3.3. Uncertainties/risks	/

4. Impacts of the options

4.1. Impacts of the options (qualitative analysis)

The positive or negative impacts from the option are derived by comparing the option against the baseline.

The positive or negative impacts from the option are derived by comparing the option against the baseline.

Category of stakeholder		*Option 1*	*Option 2*
Railway Undertakings (distributing keys)	Positive impacts	Reduced risk that fake carriers steal ticket sales revenues from them (at least for those tickets issued based on keys which were distributed via TAP TSI architecture)	as Option 1
	Negative impacts	Very limited additional costs concerning the distribution of keys Residual risk, that fake keys are still distributed within the railway sector to TCOs and used to issue fake tickets. (tickets issued based on keys which were distributed outside TAP TSI architecture)	Higher distribution costs compared to Option 1 due to creation of security certificates. This residual risk is not existing as the certificate guarantees authentity of the ticket.
Railway Undertakings (receiver of keys for ticket control)	Positive impacts	Reduced risk of revenue losses from fraud tickets of passengers	as Option 1
	Negative impacts	Residual risk, that fake keys are used by TCOs. (tickets issued based on keys which were distributed outside TAP TSI architecture)	Residual risk in Option 1 is completely mitigated. Potential impact to ticket control devices related to the security certificates
Citizens	Positive Impacts	Reduced risk to buy fraud tickets	The residual risk in Option 1 is completely mitigated.
	Negative Impacts	N/A	N/A

	Ticket Vendors/ RUs/ Third Parties (issuer of the tickets)	Positive Impacts	N/A, issuer trusts and uses his own private key.	N/A, issuer trusts and uses his own private key.
		Negative impacts	Very limited additional costs concerning the distribution of keys	Higher distribution costs compared to Option 1 due to creation of security certificates.
	Overall assessment *(input for section 5.1)*	Positive impacts	Reduced Risk of fraud tickets. Revenues from ticket sales not impacted by fraud tickets	as Option 1, however risk of fraud tickets completely mitigated
		Negative impacts	Limited additional costs for distribution of keys	Additonal costs for distribution of certificates.
4.2. Impacts of the options (quantitative analysis)	A quantitative analysis is not possible because all impacted stakeholders were not able . *to quantify additional cost impact due to distribution of keys or certificates* . *to quantify benefits resulting from risk reduction resulting from reduced ticket fraud.*			

5. Comparison of options and preferred option

5.1. Effectiveness criterion (options' response to specific objectives)

Based on the provided feedback by stakeholders the proposed options response to the specific objectives (SO) as follows

(score 1: lowest response // 5: highest response)

	Option 1	Option 2
SO A To keep the risks of frauds in the framework of distribution of tickets and ticket control to an acceptable level.	3	5
SO B To design a cost efficient public key infrastructure suitable for existing fulfilment means (e-ticket) however open for new fulfillment means such as chipcards	4	3
Total	7	8

5.2. Efficiency (NPV and B/C ratio) criterion

N/A as no quantitative data is available.

5.3. Summary of the comparison

Only Option 2 fully addresses the risk of ticket fraud, however the cost impact related to the public key infrastructure for the railway sector for option 2 is higher compared to option 1.

5.4. Preferred option(s)	The proposed option is Option 2 as it removes completely the ticket fraud risk. However it causes a higher cost impact (compared to option 1) for the railway sector due to IT costs for issuing certificates.
5.5. Further work required	N/A

6. Monitoring and evaluation

6.1. Monitoring indicators	N/A
6.2. Future evaluations	N/A