

Questions- Answers - Market Consultation Document



Project: KMC
Date: 5/28.2020
Version: 1.0
Participants: All

No	N/A	Paragraph	Questions Participants	Date	Answer
1		General	Are there requirements within ProRail for the type of key algorithm used for the keys to be managed?		see the TSI subsets 38, 114, 137
2		General	Is it a requirement, as stated in the European specifications, that PKI is used for online key management to, for example, set up TLS connections between the central systems and the key holders, such as trains?		Yes.
3		General	Should a TLS connection also be set up between ProRail's key management system and other key management systems?		Yes, There should initially at least be a connection between the key management system of NS and of ProRail. Other connections will be needed as soon as other parties implement online key management.
4		General	How are certificates currently requested, distributed and managed? Does distribution to the key holders take place via a GSM-R connection?		Currently, only offline procedures are used. GSM-R is not used for key management.
5		General	Is the management of the certificates and the internal PKI for the online connections for key management also in-scope for this market consultation?		Yes. At least the part where the online KMC application has to interface with the PKI infrastructure. Whether the rest of the PKI infrastructure will be part of the scope of the bid is still under consideration.
6		General	If it is not in-scope for this market consultation, is the management of the certificates and the internal PKI for the online connections for key management in-scope for the total solution for ProRail / ERMTS?		Yes, PKI is in scope for the total solution.
7		Legal	In what detail you intend to include answers of the participants? Would this include e.g. possible ways to continue, concepts pertaining to system architecture approaches, etc.?		Initiators will draft an overall report of the main points based on the outcome of the questionnaire. This report will be made public. Furthermore, initiators will draft a summary of all of the possible individual in-depth market consultation meetings. This summary will also be made public. As stated in the market consultation document, all information will be made anonymous and without any commercially sensitive details.
8		2.2.1.1	Are there specific Hardware and/or OS preferences at ProRail and NS?		Redhat Linux, Windows and other OS are an option. NS and ProRail prefer Redhat Linux on virtualized servers. Preference is also dependent on what we learn from the market consultation.
9		2.2.1.4	Based on the indicated TEXT-LENGTH the TEXT itself can be parsed according to this memo, KMC solution must be expanded to include the according trackside information per RBC . From our view, the information in the optional text field must influence the other messages, is this correct?		We expect the request to be executed according to the operational rules that would also apply to other non-automated requests. After the request is accepted there will be keys generated and exchanged, this will be done with other messages. These will be identical to other non-automated requests. What kind of influences in other messages are you referring to?
10		2.2.1.5	To be able to give a good estimate on the price for the KMC solution, we would roughly need the number trains /tracks in need of the solution.		Roughly 1000 trains / 100 RBC's. However, it seems artificial to make the price dependent on the number of trains as the number of trains hardly affects software complexity or maintenance cost.
11		2.2.1.8	As the intellectual Property of the current solution KEY.connect belongs to ÖBB, there are two possible ways of offering a product to ProRail. First, a license to ProRail of the 2008 product. Second, rebuild the application on a state of the art stack and allow ProRail exclusive rights. Our cost estimation based on the proposal equals, would ProRail agree to the second approach?		ProRail and NS prefer to be free to adapt/adjust the system. Other options are open.
12		2.2.1.8	What is meant by the term 'quality responsibilities' in this context?		In general any responsibility pertaining to issues with application quality: for example: who is responsible for monitoring, incident registration, software bugs, security weaknesses, interface problems, analysis of recurring problems, patch creation and installation?
13		2.2.1.10	What approach is preferred: one solution with configurable role at install time? Or two different solutions for each case?		This depends on the exact scope of the actual tender (as the different products may be separate tenders). If they are granted to the same supplier, we prefer a shared code base, and configuration at install or delivery time. Modularity might help to keep the need for frequent updates low.
14		2.2.1.10	Whats is the factual technical difference?		That depends on implementation. In principle the same KMC could be used for key mgt. in infrastructure and trains. However, if responsibilities are separated then one KMC could be optimized for key mgt. in infrastructure and another for key mgt. in trains. There are minor technical differences w.r.t. distribution to RBC and OBU and these can be found in the TSI subsets. User interface may be quite different due to different operational needs.
15		2.2.1.11	Does the application need to meet a certain Security level according to a standard (for example 62443 3-3)?		Apart from the subsets the product will also have to satisfy req at least f.e: EC 62443/ ISO27001. Exact 62443-security level is not yet defined, we currently aim for level 3. A product standard that may be a candidate is FIPS 140-2 or 3 (tamper responsive?). We are interested in the market's view on what is needed.
16		2.2.1.11	Are there specific customer requirements related to Cyber Security standards?		Most important to us is that there is a risk based development process that is completely transparent to the customer. It may be beneficial if the developer is certified. Process standards that one may think of are ISO 12207, ISO 25010, ISO 27001, ISAE 3000, ISF secure development framework, ISAE 3000, ISO 15408, IEC 62443 3-2, 4-1, TS 50701 (CENELEC WG26). For the KMC-KMC connection we wish to use a generally accepted Certificate Authority that complies with the ETSI TS 101456 standard or an equivalent standard. Apart from the subsets the product will also have to satisfy requirements, but these are not yet finished. We aim for compliance to IEC 62443, security level 3. A product standard that may be a candidate is FIPS 140-2 or 3 (tamper responsive?). We are interested in the market's view on what is needed.
17		2.2.1.14	End-users only from ProRail and NS side or also other parties, like fleet operators?		That would depend on the scope of development. But all 3 parties should be possible.

No	N/A	Paragraph	Questions Participants	Date	Answer
18		2.2.1.14	customer asks for a joint approach to develop the HMI. Does the customer have interest in own development activities or is the focus in		Both options are on the table.
19		2.2.1.16	Do you refer to a certain account directory type?		Active directory or LDAP
20		2.2.1.17	Please provide how are keys organized at ProRail and NS. Do you use a UNISIG structure?		The basic key data is what is required by the UNISIG subsets. However, there may be additional information stored. This question is focussed on the possibility to do an import, the exact format is something to be developed.
21		2.2.1.19	What does sufficient quality? What certification level does the random number generator need to meet?		Exact 62443-security level is not yet defined, we currently aim for level 3. The random number generator should be in accordance with this level. We would like to know what the market proposes.
22		2.2.1.20	Can you provide an overview of ProRail and NS server platform?		See (1.) the answer about technical preferences. Solution must also support other platform for parties outside ProRail and NS.
23		2.2.1.20	Which hardware/software platforms do you use /expect?		See answer Question 2.2.1.1 (Q: 1)
24		2.2.1.25	Are there any proprietary interfaces to be supported? Beyond the standards mentioned in 2.1.4.		For new systems only the interfaces according to subsets. However for interfacing with existing/legacy systems there may be additional interfaces required.
25		2.2.1.26	Are there any proprietary interfaces to be supported? Beyond the standards mentioned in 2.1.4.		For interfacing with other KMC's, only subsets 38 and 137 and the extension mentioned in 2.1.4 are required.
26		2.2.1.26	Is there legacy equipment in usage and if so, are Subset-conform KDCs from suppliers available?		There is equipment from different train/obu/rbc manufacturers in use for offline key management. This equipment does not perfectly fit the subset specifications.
27		2.2.1.27	Is it meant here, that specific filter criterias for the keys that are managed by the KMC are met? If yes, then all OBUs can be listed and the status of the according keys regarding OBU and RBC can be filtered. Various kinds of filtering is possible: OBU name, OBU holder, validity-period, RBC name, etc.		The question is about consistency between different locations of data storage: in the central KMC application, and the decentralized RBC's and OBU's. It is not clear how filtering functionality would address this need.
28		2.2.1.28	What is meant by "train types"?		Trains types: Train registered different train models possibly same manufacturer. (see also ERATV website https://eratv.era.europa.eu/eratv/)
29		2.2.1.29	Should it be possible here, to migrate data of other KMC (independend of supplier) to the current KMC solution?		yes, The keys that were loaded with other tools must be known to the new centralized application.
30		2.2.1.31	Does this mean, that it should be possible e. g. to require keys for a specific OBU via a specific text in an email, that can be processed by the KMC?		No, current practice is that the offline keys (subset-038 messages) are distributed by email. This question relates to integrating email distribution in the application. There is no need to automatically process email-requests, this will be an operators task.
31		2.2.1.31	What is meant by 'using functional mailbox for manual key request'. Does this mean key requests shall be received via E-Mail and then imported automatically by the KMC?		See answer Question 2.2.1.31 (Q: 21)
32		2.2.1.33	Not sure what the question is, explain more please.		For example: Non ProRail or NS parties are looking for a shared /hosting service or other services supplied. Key Management as a Service
33		2.2.1.33	What does key loading in this context mean? The current KMC solution offers different statuses for a key, e. g. requested, downloaded, installed, deleted, etc. Keys are loaded via specific online interfaces to the RBCs, where they are "loaded". Is this meant by an "operational service"?		Key Management as a Service, Shared service solution option. Everything after key creating by ProRail at least for online or even manual offline (if possible)
34		2.2.1.34	Not sure what the question is? What does "these cases" refer to? And how are we, as a vendor, involved in the operational maintenance? Or does this refer to the hosting provider? When so how does this relate to 2.2.1.20		For example: Non ProRail or NS parties are looking for a shared /hosting service or other services supplied. Key Management as a Service "these cases" refers to 2.2.1.33
35		2.2.1.35	Not sure what the question is? What does ProRail mean with a "single data model"?		All Parties NS, ProRail and others: A single data model for both offline and online keys, regardless of the responsibilities of the KMC operator (infra or train) and regardless of the method of key distribution (online/offline).