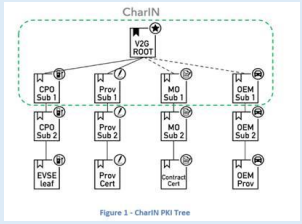
Document: FAQ_RFP_CharIN_V2G PKI trust anchor_v01
Content: Bidder questions regarding the RFP "CharIN V2G PKI trust anchor"
Version: 1.0
Provided by: CharIN e.V.
Author: Bonjad Satvat (Project manager) |pnc.project@charin.global

No.	Topic	Question	Answer
1	General	Could you please confirm if this hierarchy is expected to bear solely public trust and to trace back to one of the PKI operator's public root?	Yes, the hierarchy is expected to bear public trust, but only for a particular purpose described in ISO 15118. E.g., between chargers and electric vehicles, The hierarchy must be traced back to CharIN's public roots (V2G QA or V2G Prod).
2	General	Could you please clarify whether this hierarchy is meant to be solely operated and maintained on the side of the Certification Authority (here *Bidder*)? a. By operated is meant notably: i. All root, intermediate and issuing CAs being hosted and maintained by *Bidder* ii. Issuance of certificates iii. Acting as a registration authority	i. CharIN does not intend to host the Certificate Manager and HSM devices. It is expected that the PKI Provider offers a solution, including hosting. In this case, the PKI Provider can host and maintain all roots, intermediate and issuing CAs. ii. Although the current project scope is limited to the V2G Root and Sub CA Level 1, if it is necessary, CharIN can also consider operating the Sub CA level 2 and interfaces required to sign the leaf certificates by Sub CA level 2. In this case, the PKI operator will be the operator for the certificate issuance. iii. But, as mentioned in chapter 3.6 Setup a PKI Organization, depending on the offers and decision made by CharIN, the staffing (Registration Authority) can be in or outsourced.
3	General	Is the scope of the RFP strictly limited to the V2G Root and Sub CA Level 1, as mentioned in Figure 1 (herebelow), where the scope is given by the green dotted line  Figure 1 - CharIN PKI Tree	Although the current project scope is limited to the V2G Root and Sub CA Level 1, if it is necessary, CharIN can also consider operating the Sub CA level 2 and interfaces required to sign the leaf certificates by Sub CA level 2. Please provide information for operating Sub CA Level 2 and necessary interfaces to sign the leaf certificates of the consumers (e.g., EST or similar). Please see chapter 3.4 Operation.
4	General	Or if the scope shall include as well the operation of a PKI for V2GRootCA, SubCA level 1, SubCA level 2 and all leaf certificates, as mentioned on page 13. In this case, is the business operation (such as verification of individual and company identity, similar to KYC (Know Your Customer) operations) excluded?	CharIN is not decided yet if the necessary business operations will be outsourced to the PKI Operator or insourced by CharIN employees. Please provide information for both cases, as mentioned in chapter 3.6.
5	General	Can you provide expected Volumes of Sub1CA, Sub2CA, (and eventually leaf certificates)?	The current project scope is limited to only the V2G Root and Sub CA Level 1. If it should be necessary, CharIN can also consider operating the Sub CA level 2 and interfaces needed for issuing the leaf certificates by Sub CA level 2. **Please note that expected volumes are very uncertain at the current stage and highly dependent on factors like market development, regulations and more. But to give you a first rough indication, you can work with following estimations:** Expected volumes of each CA and lead certificates can be as follows: - CPO Sub CA level 1: one, with the renewal every four years - CPO Sub CA level 2: one, with the renewal every two years (excl. Cross Certification, signing CPO Sub CA level 2's for 3rd parties). - EVSE leaf certificates: first year, 20.000 leaf certificates (5.000 x 4, with three months renewal time) up to 100.000 leaf certificates per annum, after five years - Prov Sub CA level 1: one, with the renewal every four years - Prov Sub CA level 2: one, with the renewal every two years - Prov leaf certificates: min. four leaf certificates, up to 12x per annum after five years. - MO Sub CA level 1: one, with the renewal every four years - MO Sub CA level 2: one, with the renewal every four years - Contract leaf certificates: first year, ten leaf certificates up to 100 leaf certificates per annum, after five years - OEM Sub CA level 1: one, with the renewal every four years - OEM Sub CA level 2: one, with the renewal every four years - OEM provisioning leaf certificates: first year, ten leaf certificates

6	General	Do you expect for the operations (SubCA) the supplier to provide APIs or do you expect manual operation?	CharIN does not expect to provide APIs for the V2G Root (offline) and Sub CA level 1. An administration UI must be provided for the Sub CA level 1. In case of a necessity, CharIN can consider providing APIs for the 3rd parties, e.g., RFC 7030. For this reason, please provide technical, operational information, and costs of providing APIs for the Sub CA level 2.
7	General	Could you explicit the operation administration flow (Registration Authority…)	The processes, such as inital identity validation, identification and authentication, are currently not defined. CharIN aims to define processes in the CP and CPS documents comprehensively, which is also part of the RFP (Please see the chapter 3.3 Documentation).
8	PKI	CharIn RFP document section 4.1, the text is copied in the following : "In case of a cross-certification, the Certificate Manager Software must support the use of Subject Directory Attributes (SDA) extension with "dnQualifier" set to "CROSS", "Naming Constraints" and "Policy Constraints" according to RFC 5280 to restrict the use of cross-certificates during the verification processes." - From our understanding, o SDA contains the following attributes : Date of birth, Place of birth, Gender, Country of citizenship, Country of residence. o SDA doesn't include the dnQualifier which is more a Subject Distinguished Name's attribute. - So, we are allowing ourselves to interpret the sentence as following: o The RFP uses the dnQualifier in the Subject DN to distinguish the CA which issues the certificate. For example, ▪ For a CPOSubCA2 certificate of CharIn, the Subject DN would be : CN=CharInCPOSubCA2,O=charin,C=de,DN=charin ▪ For a SECC certificate issued by CPOSubCA2 of CharIn, the Subject DN would be : CN=SECC1234500001,O=charin,C=de,DC=CPO,DN=charin, ▪ A CPOSubCA2XS certificate is a CPOSubCA2 certificate cross-signed by a partner, the Subject DN would be : CN=CPOSubCA2XS,O=charin,C=de,DN=CROSS o The RFP uses the Name constraints in the CPOSubCA2XS to constraint that no leaf certificate can be issued by a CPOSubCA2XS cross-signed by a partner CA can be validated	Sorry for any inconvenience caused by the unprecise sentence. As you mentioned, SDA doesn't include the dnQualifier. The certificate manager software can process all the extensions described in the RFC 5280, including Subject Directory Attributes (SDA), Name Contrains, Policy Constrains, to ensure the future compatibility of the system for the new ISO 15118 standards. The subject DN examples are listed below: - CPO Sub CA level 2: DN: CN=CPO Sub CA 2, O=CharIN e.V., C=DE, DC=V2G* - SECC / EVSE leaf certificate: DN: CN=SECC12345678, O=Charin e.V., C=DE, DC=CPO - CPO Sub CA level 2 XS: DN: CN=CPO Sub CA 2, O=Charin e.V., C=DE, DC=V2G*, DNQualifier=CROSS *Domain Component (DC) attribute in the CPO Sub CA level 2 is optional in the ISO 15118 standard, and it is not defined, which values are allowed to be used as DC. The "V2G" value is used in an existing CPO Sub CA level 2 of a different provider. To avoid any unexpected issues, the same value can also be used in the CharIN PKI. The answer of your second question will be delivered after the feedback of the ISO 15118 group.
9	General	With regards to 3.6 Setup a PKI Organization, would you be able to elaborate further on what you expect here ? For example, what the roles described concretely will be expected to do etc.	CharIN does not have any experience to operate a PKI, and currently, it is not decided if the necessary organization to govern the PKI should be under the roof of CharIN. But in both cases, insourcing and outsourcing, at least the following roles are foreseen: - Registration Authority: Responsible for receiving and validating requests for digital certificates, verifying the requestor's identity. - Certificate Authority: Issuing the certificates. - Security Officer: Security policy management, security management, personnel security, physical and environmental security of the - CA/CM Administrator: Performing CA operations in the Certificate Manager software, e.g., signing, revoking, creating CRLs.
10	General	Regarding ISO 27001 certification: *Bidder1* , which was split off from its parent company *Bidder2* , is currently in the process of obtaining its ISO 27001 certification. *Bidder1* certainly expects to obtain certification by the time the project starts in August 2021 (per the RFP), but we will not have it by the time the bid is submitted. Will this be a problem? If this does present a problem, *Bidder2* received ISO 27001 last year, and we can submit the bid in *Bidder2* 's name. However, as you can imagine, we'd prefer to submit in *Bidder1* 's name. Please advise.	The submission by the subsidiary is fine, but has to be ensured and must be proven afterwards. Otherwise, this could be a reason for early termination of the contracts.
11	General	Where will the cloud server have to be located to satisfy the requirements inherent in the RFP? We assume that it will have to be in Europe? Will it have to be in Germany to be in the same country as CharIN? Please advise	CharIN prefers to have the solution in the EU or UK, but not necessarily in Germany.
12	General	If we submit a bid in line with *Bidder* providing the SubCA1 services, will our staff need to be in Germany/Europe? Or can we monitor and service from South Korea?	The location of the staff is not important for the bidding process, as long as the service levels can be guaranteed by the PKI Provider. E.g., support response times.
13	General	Will the SubCA1 services need to be 24/365? Or will it just be operational during business hours in the region where the servers are?	The PKI provider should focus on providing better SLAs; although no working hours are defined, CharIN expects to see short response times, especially for the tickets, which are categorized as critical.
14	Setup of PKI organization - 3.6	For the outsourcing aspect: Are there any minimum expectations for the roles, like for example minimum 1 FTE (Full Time Equivalent) for Head of PKI, or can individuals have multiple roles in this context?	No minimum expectactation exists, as long as the continuity of the operation can be guarenteed by the PKI provider.
15	Operation - 3.4	What is the leaf certificate revocation process accepted by CharIn? Is it a manual revocation or other process need to be done?	If CharIN decides to operate a Sub CA level 2, the recovation of the leaf certificates will be manual. But a process needs to be defined in the CP and CPS documents, incl. Circumstances, requester, procedure.
16	PKI	What are the requirements in terms of sizing of the PKI initially (Pilot project) and projection in future? (How many vehicles / charging point Operators / charging stations)?	Please see question 5.

17	General	Do you allow the bidder to answer with a partner?	Yes, the PKI operator can prepare the proposal with a partner.
18	General	Do you allow several Sub1 per type, such as several CPO Sub 1, several Prov Sub1…, or do you limit to one Sub 1 per role?	Only one Sub CA 1 level per role is forseen.
19	General	• It is not clear, if the project is about setting up V2G Root CA and SUB CA1 Level or the whole tree including leaf certificate level o WP 3.1 Clearly stated to create just a SUB CA 1 layer, in WP 3.2 its required, that an EST-interface and possibility of revoking of leaf certificates is provided	Although the current project scope is limited to the V2G Root and Sub CA Level 1, if it should be necessary, CharIN could also consider operating the Sub CA level 2 and interfaces required to sign the leaf certificates by Sub CA level 2. Because of this reason, the RFP asks the PKI Providers to deliver solution possibilities for both cases.
20	General	Being ISO15118-20 ready is just best guess so far, as the final version of the standard is still not yet published (Page 17)	The ISO 15118 Group provided certificate templates to be used as a basis in the RFP process, which will probably not change until the release.
21	General	What is happening if the Charin is using the early cancelation as listed in page 19, chapter 6 – is the supplier is paid for the planned period?	In case of early termination the cause needs to be evaluated. Dependent on the cause a potential early termination fee needs to be negotiated. See also page 19, chapter 6, item 5: "Quotations should include the option and the conditions of termination by CharIN e.V. at any stage."
22	Security	SHA1/SHA70 is officially categorized as an outdated security standard and got replaced by different other standards – why relying on such a low security level? Is this a mistake?	An equivalent and recognized alternative is also acceptable.
23	Security	One request is, to do administration over the Internet – this would create additional security risks, therefore we recommend accessing the Certificate Systems not from the Internet, an ideal/recommended setup is to operate a ceremony room to do any kind of ceremonies for all levels - this provides the needed and desired security aspect (As mentioned in the CharIN Provisioning certificate and ISO27001)	CharIN does not intent to proceed any operation regarding the root-related processes via the internet. All root related operations must proceed in a ceremony room.
24	PKI	Is there a specific preference for Offline or Online Root CAs (QA / Prod), this is not clearly stated?	As mentioned in the chapter 3.1, CharIN prefers to operate the Roots offline, both in QA and Prod stages.
25	PKI	Adding CRL and OCSP Responder to the certificates Chapter 3.1 o Adding all attributes leads to large Certificate sizes o The standard defines a maximum of 800bytes, as written in the IS=15118/2 standard o It is recommended to just use one option of revocation information	This specific issue (800 bytes vs. 1 KB) caused problem only in a specific implementation. The existing certificates are over 800 bytes in .pem coding and under 700 btes in .der coding.
26	PKI	The Certificate Profiles does not comply with ISO15118-2:2014 o mostly the attributes of the SUB CA1 are wrong – what is the expectation of CharIN	CharIN is aware of the typos in the certificates templates of the ISO 15118-2, which are not relevant for signature, cryptographic algorithm or parameters. These will be corrected and provided before a key ceremony.
27	PKI	There are a lot of optional attributes (as the standard keeps it open) o Charin needs to define them here as it needs to be clear in the setup, what needs to be supported o *Bidder* can provide a recommendation if desired	The final version of the certificate templates will be provided by CharIN after the RFP phase.
28	PKI	MO Root CA / OEM root CA o The SUB CA 1 of OEM and MO need to be derived from the V2G o The certificate templates do show a definition of a MO Root CA and OEM Root CA o How to take this into account in the proposal?	As mentioned in the Figure 1 and Figure 2, the MO and OEM Sub CA level ones are also the focus of the RFP.
29	V2G Root Key Ceremony – chapter	• Just V2G Root CA and SUB CA 1 Level requested	Please see the answer of the question 19.
30	V2G Root Key Ceremony – chapter	• No Setup of Sub CA 2 Level needed – is this right?	Please see the answer of the question 19.
31	V2G Root Key Ceremony – chapter	• OCSP is not stated in Chapter 3.1 o It is just CRL stated o Chapter 3.2 states a OCSP Setup o What is the specific request of CharIN	The OCSP responder is part of the RFP.
32	Plattform Setup - 3.2	• Revocation of Leaf certificates o In the root ceremony no Sub CA2 Level is asked - so the setup of 3.1 does not need a leaf level revocation option – is this right?	Please see the answer of the question 19.
33	Plattform Setup - 3.2	• Operation a OCSP and CRL Server included? o Running a OCSP and CRL Service is not described in specific (Page 11 - "Configuartion of the OCSP Responder") o Is this part of this request?	The OCSP responder and CRL distribution point are part of the RFP.
34	Plattform Setup - 3.2	• EST Service is requested o Without a SUB CA 2 this service is not possible	Please see the answer of the question 19.
35	Plattform Setup - 3.2	• EST after RFC7030 o Which Service shall be supported? - all or just CACerts and Simpleenrollment	At least the cacerts and simplenroll interfaces must be provided by the certificate manager system.
36	Documentation - 3.3	• Audit of CPS after independent Part – who is rated as an independent auditor by CharIN?	An independent group in CharIN will review the documents.
37	Operation - 3.4	• Renewal of OCSP AND CRL? CRL is not mentioned	Renewal of OCSP signer certificate and creating CRLs are logical part of a PKI operations.
38	Operation - 3.4	• A Charin admin shall perform the signing of a SUB CA 2 o this should be done in a secure environment - will charin admins is willing to travel to enable this phyiscally	The PKI provider must ensure a security communication between the admistrator and certificate manager system.
39	Testing - 3.5	• Testing of properties V2G Root and SUB CA1, OCSP and CRL of it?	Please see the answer of the question 19.
40	Testing - 3.5	• EST Interface for Leafs? In that case a SUB CA2 is needed, s. questions above	Please see the answer of the question 19.

41	General	You stated multiple cost-related statements: “The quotation shall consider the costs of each item separately in the work packages section”; “Each work item and additional tool shall be quoted separately”; “The quotation shall contain a clear presentation of all services rendered on an hourly basis/daily base.”; “The quoted price shall be based on these services.”; “All costs shall be planned per task of each work item.”; “A monthly report shall show all activities and related costs.” 1. What is your intent behind this request? 2. Do you intent to only contract services on a time & material basis? 3. Would you like to receive bids on only one or a few of the work packages? 4. Would a quotation based on a deliverables / fixed price item or applying a volume-based business model, without the requested breakdown of cost on a per hour basis be acceptable to CharIN? 5. Are you planning to contract for the full package or for individual work streams? 6. And / or are you planning to contract different work packages from different suppliers?	1. The aim of the separation of each work package/item is to reach a clear representation of the cost structure and transparent comparison of different offers. 2. No, CharIN does not intend to contract only time and material basis. 3. We would like to receive bids from the PKI Providers, which covers the work packages as much as possible. 4. Both are acceptable for CharIN 5. To reduce the complexity on the business side, the preferred solution would be only one contract partner. But, until the deadline of the RFP Phase, we cannot estimate if the offers will cover all the work packages. In this case, contracting multiple suppliers for individual work packages can be a solution. 6. See above.
42	General	“A monthly report shall show all activities and related costs.”. • Would this report refer to a planning in the bid or a report during execution?	The report refers to the execution phase for the selected PKI operator.
43	General	“The quotation shall be valid for the service period of 01/08/2021 for 36 months. CharIN reserves the right to postpone the start date after consultation with the PKI provider. In case of a postponement, the service period of 36 months applies from the postponed start date.” 1. What factors other than the time to go live based on development / preparation / implementation provided by the PKI provider could be a reason for postponing the start date by CharIN? 2. What is meant by postponing the start date? Please clarify if this is the start date of the project, the go live date of the PKI operation, or anything different?	The start date is referring to the start of the project. Reasons for postponement may include, for example, a delay in the procurement and ordering process or in the RFP process.
44	General	“The quotation shall consider travel costs if needed.” 1. The contracting entity will be with CharIN in Germany, however where will the CharIN team that requires travel to be located? 2. Are there physical locations to take into account in our RFP submission?	The contracting entity is CharIN Germany, with offices in Berlin. No other location needs to be taken into account for the RFP.
45	Tender process	“Bids […] will be checked with regards to their basic suitability of the bidding party.” 1. What do you mean with this check – what will be checked?	The project aims to select a PKI provider capable of providing the items listed in the RFP and has experience and enthusiasm to be part of this project.
46	Tender process	Can you provide a more detailed evaluation criteria for the responses?	The CharIN project team prepared multiple evaluation criteria with weights, such as time to go live to initial costs, security to SLA. The complete criteria list will not be shared with the bidders.
47	Tender process	“Optional: The best placed bidders will be invited to a pitch in a second process step. The order placement will be based on both quotation and pitch.” • If the order placement will be based on both quotation and pitch, how is this then optional?	In case of a close evaluation of multiple parties, the Charin Project team can invide the bidders for a pitch.
48	Tender process	“The information of the quotation is treated confidentially within the according project and the involved companies listed below:” • Is this to inform the bidding party that the information in the submission will be shared under the ‘CharIN confidential’ Confidentiality with these parties and their affiliates, or will these parties be practically involved in the evaluation process?	The Plug and Charge Project Team which currently includes the companies listed on page 9 will be involved in the evaluation process.
49	Tender process	How will you ensure that information provided in the response will not be shared with those members of CharIN that can be considered our competitors, their employees or affiliates?	An NDA will ensure the confidentiality. Only Project Team members with a signed NDA will have access to the proprietary information.
50	Work packages	3.1 Root Key Ceremony • You require SAS 70 for the root key ceremony. Would equivalent alternatives be acceptable?	An equivalent and recognized alternative is also acceptable.

51	Work packages	3.2 Platform Setup • Creation of additional subCA and cross-signing with other CAs must be possible by an CharIN admin using an interface accessible via the internet, yet section 3.1 requires the root private key to be offline. Can you elaborate on your vision how these two requirements should be combined?	Since, only the root private key must be offline, the Sub CA level 1 and 2 can be operated online. A user interface can allow the administrator to log in securely, create or import a CSR, and sign with a selected Sub CA level 1.
52	Work packages	3.3 Documentation • Please confirm Certificate Policy guideline as mentioned under 3.3. Documentation is the 'Position Paper of Charging Interface Initiative e.V., CP for ISO 15118 V2G PKI, dated 2020-08-06. • Can you share the draft CP and/or CPS?	• Yes, the Certificate Policy Guideline, which mentioned in 3.3 is the "Position Paper of Charging Interface Initiative e.V.", "CP for ISO 15118 V2G PKI", dated 2020-08-06 (https://www.charin.global/media/pages/technology/knowledge-base/78d6267a93-1615552579/charin_cp_for_iso_15118_v2g_pki.pdf) • CharIN does not have any CP or CPS draft documents.
53	Work packages	3.4 Operation 1. At 4.1.5 you list hosting 'if applicable'. Do you expect a provided solution to be turnkey, or are you open to (partially) host and/or operate a solution yourself? 2. What are requirements for validating identity and for authorizing issuance of Sub CA certificates? 3. What are the requirements for validating identity and for authorizing issuance of leaf certificates? 4. What is the expected volume of leaf certificate issuance?	1. CharIN does not intend to host the Certificate Manager and HSM devices. It is expected that the PKI Provider offers a solution, including hosting. But, as mentioned in chapter 3.6 Setup a PKI Organization, depending on the offers and decision made by CharIN, the staffing can be in or outsourced. 2. The identity validation requirements will be defined in the CP and CPS documents. 3. The identity validation requirements will be defined in the CP and CPS documents. 4. Please see the answer of the question five.
54	Work packages	3.5 Testing 1. "This work package describes the items to understand the PKI Provider's support during the testing." a. Please confirm the PKI Provider should include the end-to-end testing in the quotation. b. Alternatively, please confirm the PKI Provider should provide support to end to end testing carried out under CharIN guidance and responsibility. 2. For work package 5 (testing), do you seek independent validation as well?	1. Testing a. The PKI Provider can include the end-to-end testing in the quotation if the PKI Provider wants to offer this service/support. B. Alternatively, the PKI Provider can offer the service/support for the end-to-end testing, carried out under CharIN guidance and responsibility. 2. Yes, the project members also have experience with the PKI and the usage of V2G certificates as defined in the ISO 15118. The members are going to be part of the testing and validate the functionalities.
55	High Level requirements	4.1 Certificates 1. Section 4.1 lists TLS cipher suites to be supported by the PKI software. Can you elaborate on where you expect these ciphers to be used? 2. Which certificates you expect the PKI solution itself to use to secure the PKI solution?	1. The cipher suites are necessary for the communication between electric vehicles and chargers. Although it seems to be out of focus for this project, CharIN needs to avoid any future problems that PKI users can face. 2. It is not allowed to use certificates from the V2G certificate tree for other purposes, except the use cases defined in the ISO 15118. A separate CA is necessary for the TLS and, if applicable, authentication with a client certificate. Minimum requirements: Signature algorithm >= SHA-256, Key Size >=2048 bit
56	High Level requirements	4.2 Security 1. Are there requirements of strong preferences with respect to the country where the Root CA operates and where the Disaster Recovery system is setup (EU, US, etc)? 2. Are there any additional requirements in addition to ISO27001 (organization) and the HSM (FIPS 140-2) 3. Do you foresee FIPS 140-3 becoming a requirement in the service period (36 months)?	1. The project targets to build and operate a V2G Root for Europe. Because of this, the preferred solution and belonging disaster recovery systems should be in Europe. The selection of the country is not relevant for the assessment. 2. The ISO 27001 and FIPS level are minimum expected standards. Every higher standard is preferable. 3. Yes.
57	Legal and commercial conditions	"If the bidder is a full merchant, the contract shall be governed by German law excluding the conflict-of-law provisions. • What is the definition of a full merchant in this context? Is the equivalent of "Vollkaufmann" under German law?	The equivalent of full merchant is "Vollkaufmann" (registered merchant with business operations).
58	Legal and commercial conditions	Are there certain Terms & Conditions that CharIN would like to apply? If yes, can you please share them. If no, should the supplier propose draft Terms & Conditions?	The supplier shall propose the Terms & Conditions (see page 20 "CharIN e.V. reserves the right to negotiate the bidder's terms and conditions if necessary.")
59	Legal and commercial conditions	"The PKI provider must provide a migration plan and must ensure a smooth migration." 1. Can you elaborate on a "migration plan" and a "smooth migration"? 2. Can you specify acceptable limitations on such migration, e.g. a restriction on identical vendor HSMs. 3. Given that a smooth migration plan in part depends upon the next service provider, who will bear the costs of such migration? 4. Shall a Migration Plan be included in the response?	As you mentioned, a smooth migration can only be possible with the support of both providers. The migration will be under the supervision of CharIN to 1. CharIN expects the collaboration of both PKI Providers to reduce the complexity during a migration process. 2. Currently, there are no limitations since multiple options can be chosen, e.g., extracting the root key from existing PKI, taking the root key from backup, or setting up a new one, when the old one expires. 3. The migration cost will be calculated separately together with both providers and CharIN. 4. A high-level migration plan would be appreciated.
60	Legal and commercial conditions	Are audit logs considered data?	Yes

61	3.1 - Root Key Ceremony	The RfP states: "The Root Ceremony shall be executed according to SAS70". SAS70 was replaces with the SSAE16, which fulfils the requirements of ISAE3402. This was in the 2011. SSAE16 itself was replaced on 01.05.2017 by SSAE18. Can you verify that you want the Root Ceremony to take place according to a standard, which was replaced 10 years ago?	Yes, CharIN is expecting to see at least SAS70 procedure. All newer versions and replacements can be used in the key ceremonies.
62	WP 1.2 - Establishment of the Sub	Are the Sub1-CAs supposed to the hosted and run by the bidder or should the bidder's PKI only issue certificates for the Sub1-CAs or is it supposed to be a mix of the two options?	CharIN does not intend to host the Certificate Manager and HSM devices, and it is expected that the PKI Provider offers a solution, including hosting. The project team did not reach an agreement yet. The decision will be made before the end of the RFP phase by assessing the provided solution alternatives, including operation, hosting, SLAs, and costs. We would recommend that all the PKI providers prepare different solution alternatives they can offer.
63	WP 1.5 - Storage of Root Key	Out of the description in the RfP we assume, that CharIN wants the PKI-provider to store the root CA offline and not CharIN itself. Can you verify this?	Please see the answer of the question 60.
64	WP 1.5 - Storage of Root Key	Do you want the Root CA as well as the private key stored in a safe or is a M out of N-cards mechanism fulfilling your requirement?	Prefered solution is storing the Root CA private key in a safe.
65	WP 4.1.2 - Additional Sub 2 CA for	Are the Sub2-CAs supposed to the hosted and run by the bidder or should the bidder's PKI only issue certificates for the Sub2-CAs or is it supposed to be a mix of the two options?	Please see the answer of the question 60.
66	WP 4.1.3 - Leaf certificates	Can you describe your understanding of the leaf certificate in this project? (Especially as it is only in the CPO branch in the figure on page 14 and no leaf certificates are mentioned in the other PKI branches.) Can you give us a brief indication of the quantity model? How many leaf certificates will roughly be created, how many renewals within which timeframe?	Please see the answer of the question 5.
67	4.1 - Certificates	The TLS_CHACHA20_POLY1305_SHA256 is supposed to be used for the TLS-connection between car and charging station. Out of the RfP-description we assume, that the bidder would not be responsible for this part of the project. Can you verify this and thus clarify the need for the ChaCha20-algorithm?	Please see the answer of the question 5.
68	General	Should the proposal be in English or is German language also feasible?	The proposal needs to be in English.
69	Security	The common approach at the *Bidder* Trustcenter for a key ceremony is to follow the requirements of BSI TR-03145 resp. ETSI EN 319411-1. Is it also applicable to follow these standards instead of SAS 70?	Yes, it is also applicable to follow the mentioned standards.
70	General	Is the only main purpose of the SaaS PKI to issue Level 2 Sub-CAs or is it also planned to issue end-entitiy certificates as part of this service?	Please see also the answer of question 19
71	General	Can CharIN please provide details on the amount of Sub-CAs as well as end-entity certificates that CharIN is planning to issue and manage using the service within the 36 months of operation?	Please see also the answer of question 5
72	General	Does the "service period of 01/08/2021 for 36 months" also include the setup of the service / tenant or does it only relate to the run phase and the setup has to be finished before?	The service period includes also the setup of the service.
73	General	Is it applicable to provide for some items (e.g. license costs) a price based on the number of certificates actually being issued?	Yes, it is applicable. It should only be presented comprehensibly for us to evaluate.
74	General	Is it applicable to add or split work items?	Yes, it is applicable. It should only be presented comprehensibly for us to evaluate.
75	General	Is it applicable to also calculate costs with hourly or daily rates beside the costs for testing and external staff (e.g. work items like the support on finalizing the CP and CPS documentation)?	Yes, it is applicable. It should only be presented comprehensibly for us to evaluate.
76	General	We noticed that in one place it says "consider the cost of each item separately" and in another one/vs. "The item costs can be calculated jointly if the splitting is unnecessary." Could you please explain?	CharIN preferes to see the cost of each item separetely for a transparent assesment and easy comperation of multiple proposals. But we are aware of the diffuculty to separete the costs in some cases. Please try to separete the cost of each item as much as posibble.
77	General	What number of certificates can we assume at the beginning, or potentially for the future?	Please see also the answer of question 5
78	Tender process	"Optional: The best placed bidders will be invited to a pitch in a second process step. The order placement will be based on both quotation and pitch." Does this mean we will have the chance in such an meeting to change or expand some aspects of our quote if we will be part of the best ranked offers and because of it is described as Optional, who decides if such an Pitch Meeting will take place ?	The Project Team will evaluate the proposals of all the PKI Providers. If the evaluation results of multiple companies are close to calling a clear winner, the CharIN Project Team will invite the bidders for a pitch. Because of the current Covid situation, the Pitch Meeting will be online. Changing or expanding some aspects of the proposal would be acceptable, as long as the main solution does not change and the conditions are not worsened for CharIN, e.g., costs, delivery time, deliverables.
79	General	"The latest vulnerability assessment results, including penetration tests, must be provided to CharIN, which should not be older than one year." Does this mean you need e.g. penetration test results for comparison aspects in Phase 1 already and this is a must criterium that we need to provide such data now or is the meaning that we should or could also reflect and agree in our offer that such tests and assessments will be done in needed time frame and results can also be provided during the project ?	If a PKI Provider cannot provide security tests until the RFP deadline, we recommend companies to present a precise plan, including planned tests and their dates.