Heraklion, 26/02/2013
ENISA/ADM/DCO/dco/2013/230

CLARIFICATION TO TENDER: N^{o} 02

"Provision of Trusted Infrastructures and Services: EU Overview"

ENISA D.TCI.13.T01

Questions & Answers

Q1:	With regard to Phase 3 (as specified on p. 11 of the Tender Specification), the suggested effort (as specified on p. 13 in 4 b)) is rather limited, while the topic is quite broad. Could you give an indication of the type of output ENISA expects from this phase?
A1:	As mentioned in the proposal, the deliverable for phase 3 should be a document identifying and describing the most valuable mitigation mechanisms that should be recommended to the TSPs in order to improve their resilience and protection against the most common and relevant threats to which they are exposed. As explained in the tender specification, once known the protection mechanisms set in place by the TSPs in EU, as outcome of Phase 2, and a research of the incidents that those TSPs have suffered in the last years, this information will allow to make a risk analysis of the TSPs, regarding those vulnerabilities depending on the security mechanisms set in place, i.e. the effectiveness of them. It's not the aim of the project to be exhaustive on the analysis, but to analyse the most relevant incidents and risks in this area. This work will be done with the support of ENISA, as indicated in section 4.b), this is the reason why the effort is relatively low.
Q2:	In the ENISA Work Programme 2013 it says under WPK 1.2 that the following are considered to be trust infrastructures: - PKI and e-Signatures at national and EU level - National and cross-border eID schemes The tender specification mentions in section 1.2: - electronic signatures and electronic certificates for electronic signature, for electronic seals and for website authentication. - electronic service for trust items like: electronic seals, electronic time stamps, electronic documents, and electronic delivery. Are eID schemes to be considered in the tender?

A2:	There are other EU funded projects that have identified infrastructures from your first bullet point above. For this reason, in order to avoid overlapping with work already done, in this project will just overview these kinds of TSP, exclusively dedicated to the provision of e-ID credentials, making reference to the work already being done. This project will focus on the kind of TSPs mentioned in your second bullet point above, i.e. “electronic seals, electronic time stamps, electronic documents, and electronic delivery”. The text in 1.2 of the specification is for background information only.
Q3:	In section 2 of the tender specification e-identity trust infrastructures are mentioned. Are these the eID schemes mentioned in the Work Programme 2013 and used for eAuthentication of citizens??
A3:	No. The text in the tender makes reference to “Identify the e-signature and e-identity related trust infrastructures and service providers”, i.e. those related with the e-identity and e-signature, but without being properly them, in line with the scope of the new EU regulation on "electronic identification and trusted services" that is meant to extend the existing e-Signatures Directive to include new services such as e-stamping or e-seals that would guarantee the origin and the integrity of an electronic document. This is described in section 1.3.
Q4:	When the tender speaks of e-identity trust infrastructures does it mean eAuthentication solutions to authenticate citizens/customers?
A4:	Yes and No. The project will concentrate on infrastructures created to provide services complementary to those providing e-identity credentials to citizens/customers, as explained above. I.e. “trust infrastructures used in e-Government (e-Gov) applications in EU”, like those used in long term document storage services, or e-sealing or powers of attorney validation, but excluding the trust infrastructures exclusively dedicated to providing e-identity credentials. Nonetheless, a preliminary analysis of the market shows that many of the e-ID providers also provide complementary trust services.
Q5:	Does TSP include Identity Providers?
A5:	See replies above. Yes, only if they also provide complementary trust services.
Q6:	From the tender specification it seems on the one hand that increasing the security (especially business continuity and availability by assessment of risks and mitigation measures) is supposed to be the main result of the study while on the other hand improving interoperability between EU member states by giving guidelines is the main objective. Could you comment on this?

	How important should interoperability be in the study with respect to security? Are the risks about which the tender specification speaks, security risks or interoperability risks?
A6:	The project is not intended to go into detailed technical interoperability problems (i.e. protocols), but to administrative interoperability, i.e. administrative barriers that avoid the trust of TSPs provided from different Member States (MS), because the security measures required in one MS are different to those required in another MS. If all MS identify the same set of relevant security risks, and a harmonised mitigation strategy is defined, then those administrative interoperability barriers will lose sense and will not be justifiable. So we could summarise that this project will concentrate on those security risks that may have influence in interoperability problems, business continuity and liability are examples of them.
Q7:	In the description of Phase 1 it says: "Analyse the interfaces offered to external sources of identity". What is meant by external sources of identity? Later in the tender specification Phase 2 is described as "TSP access protocols and interfaces offered to eGov applications in EU". Does this mean Phase 2 should only cover the interfaces to (eGov) service providers? Not to the clients (users/citizens) and not to the "external sources of identity"?
A7:	Those are the two kinds of interfaces with impact on the cross-border interoperability, i.e.: a) The interfaces offered by TSPs to external sources of identity b) The interfaces offered by TSPs to eGov applications The interoperability problems to be identified are those that prevent eGov applications from trusting TSPs that don't share the same security requirements or schema. This may be due to: - lack of trust of the eGov on the TSP itself, i.e. the interface b) above - or lack of trust of the TSP on the source of identity trusted by the eGov application, i.e. the interface a) above. The title of the deliverable of Phase 2 on pg. 13 summarises both, since the interface to the external sources of identity is hidden behind the TSP interface offered to the eGov application.
Q8:	In section 2.2 on page 11 "the aforementioned questionnaire" is mentioned and also "This questionnaire could be merged with the one of Phase 1". However, there is no questionnaire mentioned earlier i.e. under Phase 1. Does this imply that ENISA intends that the survey mentioned under Phase 1 is also performed via a questionnaire?

A8:	Yes, it was assumed that the survey expected to be done in phase 1, about the basic characteristics of the services offered by the TSPs, will be done asking them some questions, i.e. using a questionnaire. The questions for phase 2 will be more technical and detailed. The rationale behind the original split of this work in two phases is that: - the information of phase 1 may be public, and known by the regulators of the MSs, so it could be collected from them. - whilst the information to be collected in phase 2 is more likely to be obtained only from direct interaction with the TSPs.