DATE: 22/03/2017

TENDER FOR KGN-SBP-04-2017

KenGen wishes to make the following clarifications as raised by potential bidders through clarification 1

Clarification 1

No.	ISSUE OF CLARITY /QUESTION	KENGEN CLARIFICATION
1	The document "*KGN-SBP-04-2017 Tender for Implementation of KenGen Digital Signature.pdf*" lacks pages 6-17.	This was a pagination error, there is no missing tender information
2	SECTION V – 1st paragraph, it's not clear who is the "*implementer*" and "*company*" – Is our understanding correct, meaning that this paragraph contents are only an introduction stating that KenGen will acquire a digital signature solution and that any future internal development shall/may use this solution?	The word **implementer** has been replaced by the word **contractor** for better understanding.
3	SECTION V – 2nd paragraph, we have elucidated that "*The solution should work with all major applications and document formats…*"	For this to be achieved the winner of this tender MUST provide an API for integration, and also to support the digital signature of documents in those formats natively or by converting them internally to a supported format. Example 1: A PDF document must be digitally signed and maintain the original document format. Example 2: It's acceptable that a TIFF document is internally converted to a PDF document to be digitally signed.
4	SECTION V – 3rd paragraph – item 3,	The solution MUST provide an API for integration with document imaging processes for electronic storage and digital signature. It's not intended to implement the scanning process.
5	SECTION V' – 3rd paragraph – item 4.	This requirement has been removed from the requirement, because KenGen already has another system for document retention rules.
6	SECTION VI' – Business Applications – item 5." This "*ADSS*"	'ADSS' has been replaced by "*solution*".
7	SECTION VI – Main functionalities expected – item 12. and 14.":	It's referred the email signatures
8	SECTION VI– Software": We will use enterprise Microsoft SharePoint portal 2007 / 2010 / 2013 connector.	For all other referred applications, an API MUST be provided for integration proposes.
9	SECTION VI– System Configuration:	a) "*ADSS*" has been replaces by "*solution*". b) SAP: An API MUST be provided by the contractor for integration proposes. However, Integration/implementation on the SAP application is not part of the scope of this tender.

		c) Installation: For clarification: the Active Directory Integration with ADSS Server should be able to provide following key services: i. Creation of user specific keys and digital certificates ii. Digital certificate re-issuance iii. Digital certificate revocation
10	SECTION VI – 3rd party Certification Authority – item 3	"*Automatic web-trusted CA* service" has been removed
11	SECTION VI – 'Must be able to use the following'	This has been revised to read: Any of these authentication Methods can be used (smartcard / token /software/ Name/Password. Biometric has been removed.
12	"SECTION VI – Signature – item 7.	"*Sectional and interdependent signatures*" has been removed.
13	SECTION VI – Signature – item 8.	"*Customizable signature block*" has been removed.
14	SECTION VI – Directories:	This part has been removed because it is covered elsewhere in the tender document.
15	SECTION VI – Security – item 1. and 4.	"*FIPS 140-2 level 3*" and "*CC EAL 4+*" are certifications for hardware security modules (HSMs). These have been replaced by "*HSM support that meet Common Criteria EAL4 and FIPS*"
16	SECTION VI – Security – item 2.	This standard is deprecated, and have been removed from the requirements.
17	SECTION VI – Security – item 3.	This standard is relative only to CAdES signature format. Therefore we have considered to include additional standards as below: (**(ISO 32000), (ISO 19005), (ETSI TS 102 778), (ETSI TS 101 903), (ETSI TS 101 733)**) (see http://www.ascertia.com/misc/signature-formats).
18	SECTION VI – Security:	We have included the standard CWA 14167-1.
19	Evaluation Criteria: Needed more clarification	1. At least two similar jobs done in two different countries supporting two different data centers. Dully signed certificates of completion for the jobs done should be provided as proof. 2. Demonstrate experience through references to have been managing/supporting data centers with at least 4 security levels and at least in two different countries. Having successfully delivered the solution in two different countries having different regulations is a proof to us that you can do the project. Remember regulations may have not been the same, which may apply to our case. This requirement is very critical. 3. Experience in implementations or hosting of server/remote signing solution for advanced signatures with qualified certificates. References must be given as proof.
20	Can you expand on **Certification Authority (CA) duly accredited by one National Security Authority**? On one hand client wants on-site PKI deployment and on the other CA accredited by NSA. This is contradictory. Further LAWtrust CAs are accredited by South African Accreditation	One of the project items is to provide Digital Certificates (see 8.1. – item 1.). These certificates are intended to be used by our internal employees and need to be issued by a Certification Authority (CA) duly accredited by one National Security Authority. Other item of the project is to deliver an in-house solution for document signing.

	Authority (for advanced electronic signatures under SA law) and by Adobe (AATL trust list). In the case these CAs are used they cannot be on-site with the client, as then accreditation would not be applicable	It will be of help to you if you try on your own to understand how digital signature works. You need the infrastructure on which to run the solution.
21	**Qualified Trusted Service Provider meaning issuing Qualified Electronic Signature Certificates and Qualified Time Stamps.** This requirement only applies to European Union, as qualified signatures are term from EU. Further, matching term in South Africa would be advanced electronic signature. Again to achieve use of such signatures, one cannot have on-site deployment of a CA/PKI.	"Qualified Trusted Service Provider", "Qualified Electronic Signature Certificates" and "Qualified Time Stamps" are European Union terms – other matching terms can be used, as long as they provide similar security and legal guaranties.
22	What is the meaning of **Certification solution duly certified by supervisor authority?**	One of the project requirements is to provide a "CA module" that in the future can be used to issue internal digital certificates. This solution must be duly certified by supervisor authority. Once again, these could be European Union specific terms, so similar terms can be used.
23	How are these requirements relevant to a signing solution? At least two (2) operations in different country's supporting different Datacenters Demonstrate experience to operate Data Centers with at least 4 security levels and at least in two different countries.	These requirements are not relevant to a signing solution itself, but are very relevant to the technical capacity evaluation of the supplier of the solution and the certificates. More explanations have been given earlier in this document under evaluation criteria.
24	When LAWtrust provides pricing, we will not include any VAT, transport, customs, withholding taxes or any other local taxes.	These are explained in the tender document please refer to the tender. I do believe that your response to the tender should include all that you think will enable you deliver the solution as required
25	Who is responsible for paying withholding tax	Please refer to the tender document and try to understand what withholding tax means.
26	Payment shall be 30days after delivery, inspection of the solution. These are not favorable payment terms	These are our terms of payment and must be followed
27	From technical specifications- The implementer shall select a third-party vendor as a "trusted certificate authority" to validate signatures. CAs do not validate signatures that is not what they do	The term is technically incorrect – we will correct it. The correct information should be "… to issue certificates".
28	The solution should allow integrating digital signatures with all manual and automated workflow and document management system to be implemented in the future. What are these all systems?	Except where otherwise specified, the solution must provide an API for future integration with those systems i.e. our systems like SAP, Workflowgen, and many more.
29	It is stated that PKI must support- Must support the following document management systems: Microsoft SharePoint Server 2007/2010/2013, K2 and Nintex Open Text (Hummingbird),	We were referring to digital signing solution, and the only required connector will be Sharepoint – for all other applications, an API will be required for future integration proposes and which must be provided by the contractor.

	Oracle, Alfresco and Laser fiche SAP, Adobe LiveCycle, Agile Frameworks, Box, Google Drive, NextDocs, Additional ECMs and industry-specific applications. This does not make any sense. PKI is standards driven and it does not support specific applications-applications must support PKI/use of digital certificates/digital signatures. If we are on the other hand talking about digital signing solution it can support integration with different applications (some out of the box and some with use of API calls etc).	
30	System Configuration and Implementation (online document signing service and ADSS configuration) What is ADSS configuration?	This has been corrected to "online document signing service and solution configuration".
31	Authentication Methods – Should authentication solution be provided or just ability to integrate?	We were referring the way users can authenticate in the solution. This item will be changed to "Must be able to use the following: User Name/Password or Digital Certificate".
32	Please clarify what do you mean by: Must support the following client OSs:	The signature solution must be compatible with end-user machines running any of the identified OSs. If the signature solution requires to install software components in the end-user machines, then that software must be compatible with the identified OSs.
33	What are non-propriatory signatures?	With a non-proprietary signature, electronic documents can be trusted and exchanged with external parties that need access to the records, entirely independent of the vendor and organization that created them
34	What are sectional and interdependent signatures	Reliance between two or more groups
35	What are invisible signatures?	It is a digital signature appearance in PDF documents (more information at: http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PPKAppearances.pdf).
36	Elaborate on Must comply with the following user directories	These requirements have been removed from the technical specifications as they are covered elsewhere in the tender.
37	Must comply with the following security standards	This requirement has been rephrased by correcting the need for compliance with some components that meet some certifications, as well removing standards that do not apply and adding some other important standards as shown below: see No. 15 1. FIPS 140-2 Level 3 validated appliance (NB: This is replaced) 2. FIPS 186 (this is removed because it is deprecated) 3. ETSI TS 101 733 4. Common Criteria EAL 4+ Certification (This is replaced)
38	What does it mean- CA solution must be able to: Lock with single CA provider?'	This has been corrected to "Not lock with single CA provider".
39	What are the local legal regulations (if these exist) in terms of accredited digital signatures?	You have to find out the local legal regulations as the bidder to be better placed for this tender

40	Would client consider off-site/cloud based solution/per user billing that will enable them to utilize AATL (publicly trusted, in the Adobe trust list) digital signatures? (Those would use digital certificates issued by LAWtrust, a company accredited under SA regulations as advanced electronic signature provider- take not that this accreditation is valid only for SA clients, as same as in Europe qualified signatures are valid only for EU based clients.)	The solution must be deployed on KenGen premises. If, on the other hand, you are referring to certificate issuance, this is a requisite, i.e., the certificates must be issued by a "Qualified Trusted Service Provider" (or other term you may use).
41	Can you extend tender submission date by 30 days	The days given is sufficient to the best of my knowledge. Please justify why you want more days.

ALL THE TERMS AND CONDITION IN THE TENDER REMAINS THE SAME

ACKNOWLEDGEMENT OF CLARIFICATION NO.1

We, the undersigned hereby certify that the clarification is an integral part of the document and has been incorporated in the tender proposal.

Signed …….

Date …….

Tenderer …….