AVOIDING THE VOLKSWAGEN EMISSIONS SCANDAL IN E-PROCUREMENT SYSTEMS: IMPERATIVE OF TRANSPARENT DISCLOSURE NORMS AND CERTIFICATION OF CRITICAL FUNCTIONALITIES

Jitendra Kohli

Jitendra Kohli, B.Tech (Electrical Engineering) from Indian Institute of Technology Delhi (IIT Delhi, India), founder of ElectronicTender, has been researching in the 'Electronic-Government-Procurement (eGP)' field for over 16-years. Based on his pioneering work, his company, ElectronicTender has developed an innovative e-procurement/ e-auction software with comprehensive security and transparency features which can be licensed for ready-deployment in any country. In public-interest, he has been sharing important aspects of his ground-breaking research in public domain through interaction with authorities in various countries (including India, EU) and multi-lateral agencies, presentation of papers at international conferences, et al, so that the concerned authorities could take appropriate measures to check malpractices under the garb of e-procurement. In end-2011/ 2012, his services were commissioned by the Asian Development Bank for technical peer-review of the update of MDB's 'e-Procurement Toolkit'. (Jitendra Kohli can be contacted at – E-mail: jkohli@electronictender.com; LinkedIn: http://in.linkedin.com/in/jitendrakohli)

ABSTRACT: The shift from manual paper-based tendering to e-procurement is now an established trend worldwide, especially for public-procurement. Technology being a dual-edged sword, it would be naive to assume that merely changing-over from manual tendering to e-procurement would eliminate all malpractices afflicting manual tendering process. In fact, unless design of e-procurement software has taken special care to prevent technology-enabled malpractices, e-procurement can be worse than manual tendering. However, if proper measures are adopted, an appropriately designed e-procurement system can eliminate/ mitigate most mal-practices. This requires that regulatory authorities in each country issue proper 'guidelines to ensure integrity in functionality of e-procurement systems', and also have reliable mechanisms to 'certify' such functionality. Further, as the 'Volkswagen Emissions Scandal' (September2015) has exposed, even certification/ testing processes can be defeated by delivering in the real-world a product which is inferior/ different from what was offered for certification. Similar

possibilities exist in e-procurement systems with scandalous implications. In this paper, the author highlights some such issues.

Key Words: e-procurement, e-tendering, public-procurement, eGP, Volkswagen Emissions scandal

.....

INTRODUCTION

The 'Volkswagen Emissions Scandal' reported in September 2015 has highlighted two unpalatable realities which have to be dealt with, if integrity is to be promoted in business environment and governance. First that even reputable organizations may sometimes cheat if they feel that they can get away with it and the incentive for doing so is high, and second that a so-called 'certified' product one may be using, could have functionality which is inferior to what the manufacturer may have offered during the certification process. So the three key-questions are,

- Is the incentive to cheat high?
- Is it possible to give one system for testing to the certification body, and deliver a different system with degraded functionality to the actual users?
- Is it possible to hide the cheating from the end-user?

The Connection to e-Procurement

If one tries to answer the three questions mentioned above in the context of e-procurement systems being used for public-procurement in various counties, unfortunately the answer for each of the questions is 'Yes'.

With typically 10% to 20% of the GDP of a country being due to Government procurement, the sinister implications of a

'Volkswagen Emissions type Scandal in e-Procurement Systems' deployed in any country can be imagined.

Hence, it is imperative to develop systems and procedures to eliminate, or at least mitigate such threats.

RELEVANT CONSIDERATIONS OF E-PROCUREMENT SYSTEMS

Advent of e-Procurement

E-procurement started getting talked about as a new methodology for conducting public-procurement circa 2000. The shift from manual paper-based tendering to e-procurement is now an established trend worldwide, especially for public-procurement. The potential benefits of e-procurement in terms of enhanced efficiency both from Buyer and Supplier perspective, as well as, increased reach are compelling. However, benefits related to enhancing Security, Transparency, Accountability and overall Integrity of the public-procurement process are contingent upon the design of the e-procurement application software, its hosting and other regulatory measures in place. Unfortunately, because e-procurement is relatively a new technology, the awareness levels amongst regulatory authorities relating to the 'pitfalls' of technology related manipulation possible in e-procurement systems may have limitations.

A Few Examples of Malpractices Possible in e-Procurement

Technology being a dual-edged sword, it would be naive to assume that merely by changing over from manual tendering to e-procurement, all malpractices afflicting manual tendering process would be eliminated. In fact, without adoption of appropriate precautionary measures, technology-enabled malpractices in e-procurement can be worse than in manual tendering. For example,

- Bid-Confidentiality can be compromised without leaving a trace in some cases
- Transparency related established practices for Public Bid-Opening can be compromised,
- et al.

The situation is compounded by the fact that in practice, many such technology-enabled malpractices may neither get discovered nor reported. Therefore, some potential pitfalls in e-procurement are such that preventive remedial measures should be taken in anticipation (Kohli, 2012, 2015).

Why the Volkswagen Emissions Scandal is Shocking

As mentioned earlier, the most shocking aspect of the Volkswagen emissions scandal is that the misdemeanour was committed by one the most reputed car manufacturers in the world. The second shocking aspect is that the vehicles in question had been duly certified by a reputable certifying body. So, if even a reputed car manufacturer can cheat, and the underlying assumptions of a reputable certification process can be deliberately compromised, then whom should the hapless consumer trust in future?

Essentially, the Volkswagen emissions scandal is about –

- a manufacturer/ supplier deliberately not deploying in the field, a product which it has got tested in the lab, or tested during inspection

- a manufacturer/ supplier deliberately not giving to a user the claimed performance or functionality, and that too after giving enhanced respectability to its claims with the fig leaf of reputable certification

- a supplier not packing in the consumer's delivery packet, products of the same quality as the samples it had shown to the consumer before the sale was made.

Related Apprehensions in case of e-Procurement

A car is at least a tangible physical entity, and if not all, at least many claims made by a car manufacturer can be verified by the user on his own, as long as these claims are 'tangible', 'physically verifiable' and 'transparently disclosed'. For example, if a car manufacturer claims that for safety it has provided four air-bags, two in the front and two in the rear, the user can actually check the provision of such air-bags.

The situation in case of e-procurement/ e-tendering can be somewhat trickier.

In the manual tendering process, if a bidder's bid-envelope was opened in an unauthorized manner before the public tender opening, the bidder can at least see with his eyes the torn or tampered bid-envelope, and protest.

In an e-procurement system, the bidder will not be able to see the tampering, at least not with his eyes! Essentially, the bidder has to trust that the e-procurement system will ensure the confidentiality of his electronically sealed-bid (ie electronically encrypted bid) till the 'Online Public Tender Opening Event'. What if this is not true, and the contents of the bidder's offer were clandestinely stolen through electronic means and shared with a competitor to the disadvantage of the concerned bidder?

Of course, there are remedial measures to eliminate such possibilities (Kohli, 2012, 2015). However, based on available information, many e-procurement systems in various countries have still not taken corrective action.

Similarly, in the manual 'Public Tender Opening Event', each participating bidder is assured about the transparency of the process with following steps:

- The participating bidders and the tender opening officers of the purchasing-entity are present together in a common room and can interact with each other during the event

- The tender-box is opened in the presence of all participants, and the bid-packets are taken out from the tender-box in front of all the participants

- Each bidder has a right to check that his bid-packet is not tampered

- Each bid-packet is opened in front of the participant bidders, so that they are assured that no document is substituted or changed

- Salient points of each opened bid are read out aloud for the benefit of all participating bidders, who are free to note the points which have been read out

- Each important page of each opened bid is counter-signed by the tender opening officers (typically there are three officers) in front of the participating bidders

- The two preceding steps ensure that no important fact or document is substituted or altered later on

- et al

It is certainly feasible to have an electronic version of the above event, with transparency related features which are equivalent or better than the manual Public Tender Opening Event as outlined above. One feature of such an electronic or online event would be that it should be conducted 'in the simultaneous, interactive, online presence of bidders'. Unfortunately, based on available information many e-procurement systems have not implemented such a transparent 'Online Public Tender Opening Event', and instead merely have an 'Online Tender Opening', which in the manual method would be equivalent to opening the bids in a room where the bidders are not present, and then subsequently displaying the opened bids to the bidders who are waiting in another room.

These are just two examples of possible malpractices. There are many more possibilities (Kohli, 2012, 2015).

INITIATING A FRAMEWORK FOR 'PROMOTING' INTEGRITY IN E-PROCUREMENT SYSTEMS

First Step

The first step in building a framework for promoting integrity and transparency in e-procurement systems would be for the concerned vigilance and regulatory authorities within a country, or at international level, to formulate detailed 'guidelines' on ensuring transparency, security and accountability in e-procurement systems. Amongst other things, the guidelines should describe the 'functionalities expected from an e-procurement system of high integrity'. Further, the guidelines should also highlight 'potential pitfalls of an e-procurement system', and make it incumbent upon the e-procurement solution/ system developers, to find suitable remedial measures to address these pitfalls while delivering the desired functionality.

It is a fact that for most end-users (viz, the Buyers and Bidders), an e-procurement system is just a 'black box'. Typically, they do not understand the technical intricacies of an e-procurement system, or how data is actually processed/ manipulated within the system.

Once a Government body recommends the use of an e-procurement system, most end-users would blindly follow the procedures in good faith. Therefore, it is duty of the regulatory bodies to ensure that e-procurement system/ solution providers develop and deploy systems of high integrity, and the end-users have reasonable awareness levels of the required functionalities. This would be possible only if detailed guidelines exist for the purpose.

India was perhaps the first country to issue comprehensive guidelines on 31st August 2011 to ensure integrity of e-procurement systems (STQC Directorate, 2011). To some extent, the author was instrumental in making the vigilance and other regulatory authorities in India aware of the need for having such guidelines. The European Commission also set up an e-Tendering Expert Group (e-TEG) for a similar purpose. The final report of e-TEG was issued in the year 2013 (e-Tendering Expert Group, 2013).

Without the existence of such guidelines, anybody can conjure up an e-procurement system and take the hapless users for a ride.

Second Step

Once comprehensive e-procurement guidelines are formulated, it would be necessary to make the guidelines mandatory and implement these, otherwise the guidelines would be nothing more than a facade. Implementation of guidelines would entail the following:

- Dissemination of information about these guidelines to various potential users of an e-procurement system, both Buyers, as well as, Suppliers/ Bidders

- Making it mandatory for e-procurement solution developers/ providers, as well as, e-procurement service-providers to be certified by a testing agency of high credibility for full compliance with the guidelines

- Ensuring that the team of the designated testing agency be fully conversant with the guidelines, as well as, the guiding principles and procedures of Public-Procurement.

India as a Role Model

India again took the lead by making it mandatory in 2012 for all 'e-procurement solutions and systems' being used in the country to be certified for compliance with its e-procurement guidelines issued on 31st August 2011 (STQC Directorate, 2011). The Central Vigilance Commission and the Finance Ministry directed that the certification be carried out by a designated testing agency of the Government of India. Furthermore, instead of concentrating all Government procurement in one centrally controlled system, a Government purchasing entity could use any e-procurement system as long as it was certified as mentioned above. The latter step is necessary to encourage innovation, dynamism in an emerging technology-based field, and avoiding having a centralised hub of corruption.

If one considers the above two achievements, India is probably ahead of the rest of the world in terms of having a framework for 'developing and deploying e-procurement systems of high integrity'. It would be pertinent to mention here that in respect of enforcement in the Indian context, some ground is still to be covered.

Other countries can consider emulating India's example in promoting e-procurement and creating the first two steps of a framework for ensuring integrity. Then where is the challenge, and where does the fear of Volkswagen-Emission type scandal arise in e-procurement?

The Challenge and Apprehension

The challenge arises because the world is not so simple that an institution makes rules of good conduct and practising integrity, and everybody happily falls in line! That would be a utopia. To have a utopian situation in the area of public-procurement where huge money is involved, would be some kind of super-utopia!

The apprehension of Volkswagen-Emission type scandal arises in e-procurement in a scenario, where an e-procurement solution/ service-provider hoodwinks the users of its system by taking 'certification' for its system for compliance with the 'prescribed guidelines', but actually deploys in the field a system with functionality which is inferior/ different from what was offered for certification.

Needless to state, the situation will be much worse in a country where there are no guidelines on e-procurement (or only some mild guidelines), and naturally no certification process for

compliance with such guidelines (or some insignificant certification process). Such systems are not even worth discussing from an integrity perspective. Taking an example from the automobile industry, it would be akin to a situation where a car is belching smoke and other pollutants with impunity, but there are no emission norms to check it. In all probability, the established manual tendering processes would have higher integrity in this situation.

EVOLVING THE FRAMEWORK FOR 'ENSURING' INTEGRITY IN E-PROCUREMENT SYSTEMS

If e-procurement is not to become a mere 'fig leaf' for hiding technology-enabled malpractices, sooner rather than later the first two steps of having appropriate 'guidelines' and 'certification' would have to get implemented in all countries where e-procurement is being encouraged. If this is not done, it would be similar to a situation where air-travel is being encouraged without having any aviation guidelines and air-traffic control. The next challenge would then be to detect and stop malafide deviation in what is deployed in the field vis-à-vis what was approved during certification.

As stated earlier, since India is one of the few countries (or perhaps the only country) to have implemented the first two steps in creating a comprehensive 'framework for promoting integrity in e-procurement systems', mainly 'case-study data' of the Indian scenario is being taken for further discussion on the subject, without naming any organization in whose system deviation is suspected.

Objective

The objective of the paper is to enhance and evolve the existing framework to a higher level, where any 'deviation from the norms' is detected and controlled. The evolved framework can then serve as a 'road map' for various countries which are serious about encouraging e-procurement for 'enhancing integrity and transparency in public-procurement', and not merely as a technology-based fad for replacing the tried and tested manual tendering process.

CHECKING DEVIATION OF CERTIFIED E-PROCUREMENT SYSTEMS WITH RESPECT TO E-PROCUREMENT GUIDELINES

There are various potential lacunae/ loopholes in e-procurement systems, which can be exploited by unscrupulous players (Kohli, 2012, 2015). In respect of the subject of this paper, two specific 'red flags' are being taken for discussion, viz – 'Encryption of Bid Data' in e-procurement systems (which is the equivalent of 'bid sealing' in the manual tendering process); and the Online Public Tender Opening (which is the equivalent of the transparent public tender opening event in the manual tendering process). Since these two aspects have critical importance in the public procurement process, the guidelines on e-procurement expectedly dwell on these two aspects in detail.

What the Guidelines have to say about Bid Data Encryption

Section 6.7 of Part-II of the final report issued by the e-Tendering Expert Group (e-TEG) appointed by the European Commission (e-Tendering Expert Group, 2013) states –

QUOTE:

6.7 Confidentiality of Tenders

Business problem/Objective: As per Procurement Directive, the platform must guarantee that no access to tender documentation can be achieved by anyone before the deadline. The challenge here is to provide a robust design so the confidentiality of the tenders is guaranteed. Mainstream approach: tenderers encrypt their tenders using public key cryptography and transmit the complete tenders to the platform. This method reasonably ensures that no one can access data transmitted before the submission deadline. In fact the process places the responsibility on the CA in charge of opening the tenders (tenders cannot be decrypted unless their private keys are used). However, *this approach does not offer complete assurance against malicious activities as the decryption keys are within the CA organisation*. Illegitimate copies of the tenders can in fact be produced and decrypted by unfaithful CA staff before the opening deadline.

Recommendation: To address the fear of EOs that the tender can be accessed by CA staff with an interest …

… *way to ensure full confidentiality is to use symmetric encryption, enforced via a tenderer generated key*. The tender is transmitted in its entirety to the platform in a scrambled format and stays encrypted until a public opening date. On the public opening date, tenderers are invited to connect to the platform and remotely

launch the decryption functionality with the key in their possession. UNQUOTE

As can be seen from the above excerpts, bid data encryption done using public key cryptography (also referred to as PKI or asymmetric key) has concerns, while full confidentiality can be achieved using tenderer-generated (ie bidder-generated) symmetric key.

The Indian guidelines on e-procurement convey the same message in a slightly different and elaborate manner. For details, reference may be made to sections 2.0, 3.0 and 4.0 of Annexure-I of the Indian guidelines (STQC Directorate, 2011).

Importantly, the Indian guidelines go a step further. Keeping in view that some e-procurement solution/ system providers have used PKI/ asymmetric key for bid encryption, the guidelines provide hints about some augmenting-techniques to at least mitigate the concerns, since these concerns about use of asymmetric key for bid data encryption cannot be fully eliminated.

Some relevant recommendations under section 2.1 of Annexure-I of the Indian guidelines are excerpted below –

QUOTE:

Guidance and recommended practices- Use of PKI technique

If the e-procurement system uses PKI for bid-encryption, it has to satisfactorily address the above issues and consequent concerns (Ref 2.2 below) through suitable functionality built into the e-procurement application. Where, in addition, some issues are being further addressed through organizational procedures under ISO 27001, these should be explicitly defined with satisfactory explanations, otherwise certification process will become subjective. While doing this, the following can be kept in view:

Various techniques are available in market for improving implementation of PKI based encryption such as escrowing, splitting and repeated encryption to further strengthening the security of information and implementation. If the e-procurement system uses any of the above techniques, it will have to be explained how the related concerns (Ref 2.2 below) have been addressed. Furthermore, practical procedures will have to be put

in place which can be implemented at the field level in diverse locations in the country in a user friendly manner.

UNQUOTE

Some excerpts of section 2.2 of Annexure-I of the Indian guidelines are as follows (STQC Directorate, 2011):

QUOTE:

While all efforts must be made to ensure that no spyware is put in the server which can make clandestine copies of a file or data being uploaded to the server, and then sending this clandestine copy to a secret destination, the possibility of such spyware being planted in the web-server cannot be totally ruled out. ...

Guidance and recommended practices- Spyware/Trojan/BOTS

It is important that even if a clandestine copy is made and stolen as above, the bid encryption methodology should be such that it should not be possible to decrypt the bids in connivance with any officer of the Buyer organization or the Service Provider organization. While this issue becomes irrelevant if bid encryption is done at bidder end with bidder created symmetric pass-phrase, in case PKI-based bid encryption is done, the software functionality has to be suitably augmented to mitigate this security threat. UNQUOTE

Further,

QUOTE:

Private Key with which decryption is done, is available with the concerned officer before the Public Tender Opening Event

a) If a clandestine copy of a bid is made as described above before the 'tender opening event (TOE)', and if the concerned tender opening officer (TOE-officer) connives in decrypting the bid before the TOE, the confidentiality of the bid is compromised.

b) The above concern with the difference that the copy of the bid is made with the connivance of the Database Administrator (DBA).

c) If the concerned TOE-officer(s) is/ are absent during the TOE, how the bids will be decrypted especially keeping in view that the private-keys should not be handed over to anybody else.

… Guidance and recommended practices

Note: While some guidance is provided below, it is the responsibility of the individual vendors to design and develop their applications in a manner that addresses the outlined concerns. …

A process needs to be established and followed in respect of key management of encryption keys particularly the key with which the bid would be decrypted at the time of opening of the bids. Such process should avoid compromising confidentiality and possibility of decrypting clandestine copy of the bid. In this regard the following three approaches may be adopted with proper checks while keeping in view the legality of the process for end-users. Furthermore, practical procedures will have to be put in place which can be implemented at the field level in diverse locations in the country in a user friendly manner.

- Splitting of Keys:

  A bidder would submit the bid document after encrypting it with the public key of the tendering organization, so that the contents are encrypted and are decrypted by the authorized officials at the tendering organization. To minimize the risks associated with "person of dubious integrity" or collusion, private key decryption should be split into `M' parts with the requirement of minimum `N' splits being required for its use. (`N' should be more than 1 and less than or equal to M). `N' and `M' will be decided by the tendering organization and suitably configured on the system.

- Multiple encryption of the bid document with multiple public keys and decryption of document with the multiple corresponding private keys of the tendering organization. UNQUOTE

Prescriptions in the Guidelines about Online Public Bid Opening

Section 7.1of Part-II of the final report issued by the e-Tendering Expert Group (e-TEG) appointed by the European Commission (e-Tendering Expert Group, 2013) states –

QUOTE:

7.1 Unlocking tender box …

Recommendation: The platform must provide functionality to ensure that at least two separate users with two different logins may unlock the tender box and decrypt the tenders. Public-key cryptography should be used to guarantee the identity of authorised users in charge of unlocking/decrypting the tenders. For top-level confidentiality assurance, the CA may require that the tenders be encrypted with the symmetric key of the tenderer and keep the tenders encrypted in the database until opening. If this is the mechanism chosen, then the opening procedure is public event (see below, 7.3). Tenderers are in fact required to take part in the process to enable opening of their own individual tenders using their deciphering key.

…

7.3 Opening notification

Business problem/objective: In order to improve transparency and accountancy throughout the e-tendering process, EOs should be able to query the status of their tender(s) in the platform.

Recommendation: The e-Tendering system should allow the CA to communicate to the EOs about processing steps of their submissions (such as opening, completeness assessment…). In some countries law defines the opening process as a public event open to all tendering organisations. Certain data on each tender must be made known to them according to legal requirements to ensure transparency. Platforms should support this legal requirement.

UNQUOTE

The Indian guidelines on e-procurement elaborate in detail on how the Online Public Tender Opening Event ought to be conducted if transparency is to be ensured. For details, reference may be made to sections 6.3 of Annexure-I of the Indian guidelines (STQC Directorate, 2011).

QUOTE:

… Guidance and recommended practices

The GFR requires that tenders be opened in public in the presence of the authorized representatives of the bidders. The Finance Ministry Manual on procurement procedures outlines in details the requirements of a transparently conducted Public Tender Opening Event. CVC Guidelines on security aspects of e-procurement also state the requirement of 'Online Public Tender Opening Event'. Merely opening bids 'online', and then separately making them available for display to the bidders subsequently, and/ or from a different location/ screen (ie user interface) without the simultaneous online presence of bidders, does not fulfill the requirements of a proper and transparent online Public TOE. A comprehensive and transparent Public Tender Opening Event is the 'backbone of transparency and fairness' of the Public Procurement process, manual or electronic. This has an impact on technical as well as procedural aspects.

It must be ensured that e-tendering/ e-procurement has comprehensive functionality for a transparent Public Online Tender Opening Event (Public OTOE). Well established practices of manual tender opening (with legal and transparency related significance) should have corresponding electronic equivalents for transparent e-tendering/ e-procurement. Some relevant processes of a fair and transparent online public TOE should include:

i. Opening of the bids in the simultaneous online presence of the bidders with proper online attendance record of the authorized representatives of the bidders. Merely opening bids online, and then subsequently displaying some results to the bidders does not fulfill the requirements of a transparent Online Public Tender Opening Event
ii. Security Checks to assure bidders of non-tampering of their bids, et al during the online TOE itself
iii. One-by-one opening of the sealed bids in the simultaneous online presence of the bidders
iv. Online verification of the digital signatures of bidders affixed to their respective bids
v. Reading out, ie allowing bidders to download the electronic version of the salient points of each opened bid (opened in the simultaneous online presence of the bidders)
vi. There should be a procedure for seeking clarifications by the TOE officers during online Public TOE from a bidder in the online presence of other bidders, and recording such clarifications

vii. Digital counter-signing (by all the tender opening officers) of each opened bid, in the simultaneous online presence of all participating bidders
viii. Preparation of the 'Minutes of the Tender Opening Event' and its signing by the concerned officers in the simultaneous online presence of the bidders

While bidders should be welcome to be present physically during the TOE, it should not be mandatory for them to do so. All the above should be achieved online in a user-friendly manner.

The e-procurement system has to satisfactorily address the above requirements through suitable functionality built into the e-procurement application. Where, in addition, some issues are being further addressed through organizational procedures under ISO 27001, these should be explicitly defined with satisfactory explanations. UNQUOTE

Expectations from e-Procurement Solutions/ Systems which have been Duly Certified as per the Guidelines, and Initial 'Indicators' of Deviation

As mentioned before, since India is one of the few countries (or perhaps the only country) to have implemented the first two steps (although enforcement of the second step is still partial) in creating a comprehensive 'framework for promoting integrity in e-procurement systems', mainly 'case-study data' of the Indian scenario is being taken for further discussion.

If an e-procurement solution/ system has been audited and duly certified as per the guidelines (STQC Directorate, 2011), it is expected that functionalities, augmentation and remedial techniques as prescribed or suggested in the guidelines should be manifest to the concerned users while using the system.

For example, the tangible steps prescribed for the Online Public Tender Opening Event (i to viii as outlined above) should be clearly experienced by the bidders in an interactive manner. If the aforementioned steps are missing during the actual opening, and the opened bids are just displayed in a single step to the participating bidders, then certainly something is amiss, and an apprehension similar to the Volkswagen emissions scandal arises!

In the manual tendering process, this would tantamount to bids being opened not in front of the bidders as prescribed, but in another room and then brought before the bidders. Which bidder will trust such a process?

Assuming that the certification process was correctly done, strictly in accordance with the guidelines, the e-procurement system provider is clearly not offering the same functionality during actual deployment as it may have offered during certification.

Similarly, both the European guidelines (e-Tendering Expert Group, 2013) and the Indian guidelines (STQC Directorate, 2011) have clearly implied that bid data encryption using bidder-generated symmetric-key has 'Nil concerns' about 'breach of bid-confidentiality'. In contrast, both the guidelines have expressed concerns if asymmetric-key, ie PKI is used for bid data encryption. As already explained before, the Indian guidelines have gone a step further, and suggested the e-procurement solution/ system provider reduces the risk by augmenting the functionality with techniques such as – Key splitting, multiple encryptions, etc.

If an e-procurement solution/ system, which uses asymmetric-key/ PKI for bid data encryption, has been audited and duly certified as per the guidelines (STQC Directorate, 2011), it is expected that the users of the system will experience the augmentation steps such as key-splitting, multiple-encryptions. If the aforementioned steps are missing during the actual process of encryption and decryption of the bids, then certainly something is amiss, and an apprehension similar to the Volkswagen emissions scandal arises!

The initial 'indicators' of deviation in some certified e-procurement systems have emerged from information available in public-domain, such as 'user manuals', and the experiences of users who have actually used such systems.

Making Detection of Deviation Easier for End-Users, the Imperative of Transparent Disclosure Norms

A deviation can be detected only if there is a benchmark for comparison. Most users of e-procurement systems are lay persons, and are not aware of the intricacies of e-procurement. They know what to expect from the manual tendering process, but do not know what exactly to expect from the electronic process. It would be normal for lay users to look at technology-based e-procurement systems with awe.

Such users would not be able to notice the missing functionalities. Neither are they aware of the guidelines. At the most, all they can see is that the e-procurement system provider has claimed that its system is 'certified'.

The situation is compounded by the fact that the 'certificate of compliance with the guidelines' (which the e-procurement service provider may have displayed on its portal) does not list out salient/ critical functionalities which have been tested, so the users are blissfully unaware of what to expect.

An important step in curbing such deviations by unscrupulous e-procurement service providers would be to empower the users with more information and disclosures about some salient functionalities. Along with the 'certificate of compliance with the guidelines' (STQC Directorate, 2011), the certificate should transparently display in tangible terms (as an annexure to the certificate), salient functionalities which have been certified relating to –

- Bid data encryption methodology and augmentation techniques used for compliance with the guidelines (with reference of corresponding sections of the guidelines)
- Online Public Tender Opening Event steps, and how a bidder can interactively participate in the online event with full transparency (with reference of corresponding sections of the guidelines)
- et al

If salient functionalities are transparently disclosed (preferably on the website of the certifying agency, in addition to the website of the e-procurement service provider), the users can find out themselves, 'what to expect' and 'what to check out' during different stages of the e-procurement process.

Once 'Transparent Disclosure Norms' are implemented as suggested above, to some extent it will improve the situation and bring it closer to the automobile industry. In the latter case, based on disclosed features, at least a prospective buyer of a car can 'check out' what features to expect in a car he or she is planning to buy – air-bags in the front and rear or only in the front, central-locking, etc.

Formal Mechanism for Detection of Deviation and Remedial Action

The aforementioned 'Transparent Disclosure Norms' will increase the awareness levels of end-users of the e-procurement system, and thereby reduce to some extent the problem of deviation by unscrupulous e-procurement service providers.

However, in general, most end-users of the system will not have the wherewithal to check out all functionalities, especially those functionalities which are not visible to the eye, or those which require special tools.

To curb deviationist behaviour amongst unscrupulous e-procurement service providers, the Government should appoint another reliable agency to do 'periodic surprise-audit' of the 'certified e-procurement systems in deployment', and check whether the functionalities and user-documentation are in full compliance with the guidelines (STQC Directorate, 2011). Needless to state, this audit agency should be independent of the testing/ certifying agency which originally 'certified' the system.

CONCLUSION

A mature and dependable regulatory framework for 'ensuring integrity in e-procurement systems' used for public-procurement within a country, will broadly have four levels as summarized below:

1. Formulation of detailed 'Guidelines' for ensuring Security, Transparency, Accountability and overall Integrity in the e-Procurement solutions/ systems

2. 'Certification of the functionalities and integrity' of an e-Procurement system for full compliance with the promulgated guidelines. A dependable testing/ certifying agency would have to be designated for this purpose

3. 'Transparent Disclosure Norms' as an integral part of the certificate issued by the certifying agency

4. 'Periodic Surprise-Audit' by an independent empowered agency –

    a. To ensure that the certification is as per the guidelines

b. To confirm that what is deployed in the field is the same as what was presumably certified (and not a diluted or compromised version)

The above suggestions are necessary if reasonable assurance of 'Integrity' is to be provided to e-Procurement systems being used for Public-Procurement. Some critics of the above suggestions may wonder whether so much fuss is required for an industry where the total revenue would be just a few billion US dollars. The issue here is not of the revenue generated by the e–procurement sector. The critical issue is that these e-procurement systems will be facilitating and processing tenders worth trillions of US dollars, 10% to 20% of the GDP of every country.

REFERENCES

e-Tendering Expert Group (e-TEG) appointed by the European Commission (2013). *Recommendations for Effective Public e-Procurement, Part II: Operational Recommendations*. [Online]. Available at http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/eteg/eteg_part2-operational_recommendations_en.pdf. [Retrieved March 30, 2016]

Kohli, J. (2012). *Red Flags in e-Procurement/ e-Tendering for Public Procurement and Some Remedial Measures*. Paper presented at the IPPC5 at Seattle, USA. [Online]. Available at http://www.ippa.org/IPPC5/Proceedings/Part2/PAPER2-6.pdf [Retrieved April 6, 2016]

Kohli, J. (2015). "Combating Organized Corruption in Public-procurement Through Appropriately Designed e-Procurement Systems''. Paper presented at the Third Conference on Evidence-Based Anti-Corruption Policies (CEBAP III) on Organized Corruption', organized by Thailand's National Anti-Corruption Commission (NACC) in collaboration with the World Bank et al., Bangkok, Thailand, June17-18, 2015.

STQC Directorate (2011). *Guidelines for Compliance to Quality Requirements of eProcurement Systems* (Issued on 31st August 2011 by the Department of Information

Technology [now called Department of Electronics and Information Technology, DeitY], Ministry of Communications and Information Technology, Government of India). [Online]. Available at http://www.stqc.gov.in/sites/upload_files/stqc/files/Guidelines-for-Compliance-to-Quality-Requirements-of%20e-Procurement-Systems.pdf and http://egovstandards.gov.in/sites/default/files/Published%20Documents/Guidelines%20for%20Compliance%20to%20Quality%20Requirements%20of%20e-Procurement%20Systems.pdf. [Retrieved March 30, 2016]