Technical Assistance Consultant's Report

Project Number: 47192-001
October 2018

Regional: Cross Border Trade in e-GP Era: Challenges & Way Forward

Prepared by

Dr. Ramanathan Somasundaram
India

For the Asian Development Bank

Asian Development Bank

DISCLAIMER

ABOUT THE AUTHOR

Dr. Ramanathan Somasundaram researched e-Government Procurement (e-GP) for his doctoral thesis work in Denmark and has more than 10 years of experience in consulting, implementation and assessment of e-GP systems.

ABBREVIATIONS

ADB	–	Asian Development Bank
B2C	–	Business to Consumer
CA	–	Certification Authority
CPV	–	Common Procurement Vocabulary
EIDAS	–	Electronic Identification and Trust Services
EU	–	European Union
e-GP	–	Electronic Government Procurement
GPA	–	Government Procurement Agreement
MLES	–	Model Law on Electronic Signatures
PKI	–	Public Key Infrastructure
TED	–	Tenders Electronic Daily
WTO	–	World Trade Organization

NOTE

In this report, "$" refers to US dollars

CONTENTS

I. INTRODUCTION

1. The shift from manual procurement to e-Government Procurement (e-GP) got off to a start in early 2000. Driven by transparency and efficiency considerations, many more countries embarked on adoption of e-GP in the subsequent decade. Thus, adoption of e-GP gained momentum across all parts of the Globe viz. North America, South America, Australia, South Asia, Asia Pacific, East Asia, Central Asia, Eastern Europe, Africa, Middle East and North Europe. Now, most countries have already implemented e-GP and the rest which are yet to implement e-GP will get on-boarded in near future. The countries which have implemented e-GP have in most cases completely discontinued manual method of procurement. A supplier seeking to respond to tenders in such countries shall necessarily submit its bid only using e-GP.

2. e-GP is comprised of a broad range of functionality covering processes under pre-tendering, tendering and post-tendering. Very few countries have had success in implementation of a full-fledged e-GP system covering end-to-end procurement flow (i.e. from indenting / work estimate preparation, tendering, contract management and contract payment management). The countries with e-GP system have primarily focused on implementation of e-Tendering. The rest of the procurement functionality gets added on the e-GP system gradually.

3. There is a large number of operating free trade agreements in the World under different categories viz. Multi-lateral, plurilateral and bi-lateral agreements. Government Procurement Agreement (GPA) is a plurilateral agreement which has 47 WTO members as its signatories. Another 29 WTO members are in observer status[1]. GPA aims to *"… mutually open government procurement markets among its parties."* And, it applies to *"… procurement of minimum estimated value equal to or exceeding certain specified financial value thresholds"* as agreed by the signatories. The size of market opportunities covered by GPA is estimated at USD 1.7 Trillion. The World Trade Organization (WTO) has set-up an e-GPA portal (https://e-gpa.wto.org/) wherein detailed information about parties' coverage commitment is provided.

4. A significant percentage of USD 1.7 Trillion covered under GPA and additional government procurement contracts covered under multiple other free trade agreements can now be accessed only using e-GP systems. Ideally, e-GP systems should have been designed to seamlessly allow business entities to participate in tenders published in the system from across international borders. In practice however, certain security and authentication framework implementation disallow or create barriers for foreign bidders in accessing e-GP system. Consequently, e-GP systems create a technology barrier in implementation of free trade agreements.

5. The need of the hour is to evolve systems that enable foreign business entities to authenticate their identity and submit their bids online in a secured manner using e-GP system. The key challenges in development of e-GP system that enables international bidding within a safe and secured security and authentication framework are explained herein. Also, this paper deliberates upon possible solutions to the challenges identified.

[1] Source: https://www.wto.org/english/tratop_e/gproc_e/gp_gpa_e.htm (site accessed on 12th of April 2017)

II. KEY CONCEPTS EXPLAINED

A. Authentication Framework

6. The agencies implementing e-GP system seek to authenticate identity of users mainly for the following reasons:

(a) Development of a reliable supplier / contractor database. If same user gets registered in duplicate, the supplier performance reports generated in e-GP system will not be faulty;
(b) Reliably associate a user registered online with a confirmedly existing legal entity. Else, there is a risk of fraudulent or fictitious users registered in the System; and
(c) Reliably attribute action taken in e-GP system to a user registered in the system. The user on a later date shall not repudiate its action registered in the system. For example, if Company A claims that it did not submit bid or it quoted a much higher amount than what is recorded in the system, there must be a mechanism to prove in a water tight manner what Company A actually did in the system.

7. This authentication of users is done online using "*Electronic Signature"* or *"e-Signature"*. Electronic Signature is defined in the UNCITRAL Model Law on Electronic Signatures (MLES) as *"… data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message"*. e-Signature is a broadly defined and technology agnostic legal concept which captures intent and consent. Whereas, *"Digital Signature"* is a type of e-Signature wherein Public Key Infrastructure (PKI) infrastructure is used to reliably authenticate user identity and strongly associate a user with actions taken online. The principles underlying e-Signature and Digital Signature are not different. However there are differences in the manner of implementation.

8. As per Article 6 (3) of MLES, "*An electronic signature is considered to be reliable … if:*

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person; UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable."

9. However, Article 6 (1) of MLES does qualify that electronic signature can be *"… as reliable as was appropriate for the purpose for which the data message was generated or communicated"*. Business-to-Citizens (B2C) e-Commerce use a certain form of e-Signature to authenticate online transactions.

10. Digital signatures require establishment of PKI infrastructure at the National level. Key highlights of PKI infrastructure are explained below:

(i) A Certification Authority (CA) authorized under provisions of the e-Signature legislation verifies identity of a person and then issues a Digital Signature Certificate (DSC) tagging a unique private-public key pair to the person;
(ii) The private key can be accessed only by the concerned user as this access is typically password protected;
(iii) The hash generated from the message content to be signed is encrypted using the private key. This encrypted hash is referred to as digital signature;
(iv) Public key corresponding to the private key can be used to decrypt the encrypted content (i.e. from cipher text to the hash value);
(v) Verification of signed data can be done as follows:
    a. Data integrity: Regenerate hash of the content and verify with the decrypted hash value. If both hash values match, it is confirmed that the content has not been altered subsequent to signing;
    b. Non-repudiation: If encrypted hash is decrypted using public key of a user corresponding to the private key, it is confirmed that the user signed the content; and
(vi) This public key is by definition freely available for the public. Hence any party can verify the signed data.

11. Digital signatures are unfriendly for international trade because a foreign user needs to prove its identity to the concerned National CA to obtain a DSC valid in the bidding country. Such identity verification creates procedural hurdles especially for foreign bidders.

12. It is a matter of choice for e-GP system designers whether to adopt e-Signature or digital signature based authentication framework. Certain countries such as Georgia and Kyrgyz have adopted e-Signature based authentication framework because it is user friendly and it allows foreign bidders to freely use the e-GP system from anywhere in the World. Digital signature based authentication framework is adopted in countries such as India, Bangladesh and South Korea. These countries prioritized stronger user identity verification and irrefutable model of associating a user to actions taken online in e-GP system at the expense of wider inter-operability and user friendliness.

13. Article 12 in MLES calls for recognition of digital signature and e-Signature with the same legal effect regardless of whether or not in signature is generated locally in the enacting State or outside the enacting State. The European Union (EU) has in 2014 enacted Electronic Identification and Trust Services (EIDAS) regulation, which has created standards for electronic signatures and qualified electronic signatures (i.e. digital signatures). Also, the regulation requires EU member States to accept digital signatures issued in any of the EU member States. The need for mutual recognition and interoperability of digital signatures across multiple countries is widely acknowledged. In due course, it is expected that many more countries will mutually recognize digital signatures issued by foreign countries.

14. The key criticisms against the adoption of digital signatures are:

(i) There are loopholes in the process adopted by Certification Authority in issuance of digital signature certificate tagging the public-private key pair to a user. Hence, they claim that the foundation underlying digital signature is shaky; and
(ii) Instead of digital signature based identity verification, purchasing agency can verify user identity during tender evaluation as pre-requisite for award of contract. The Government can exercise its rights to black-list a business entity or

confiscate bid security if a bidder repudiates its action taken online in e-GP system.

15. A key requirement underlying implementation of e-GP system is development of a National database of business entities. Such a database will enable Government to:

(i) Analyse in detail quantum of work awarded to business entity and spare capacity available with a business entity; and
(ii) Effectively black-list a business entity such that the entity is disallowed to participate in Government tenders for a period of time.

16. A key pre-requisite for development of National database of business entities is establishing uniqueness of a business entity registered in e-GP system. Neither Digital Signature nor e-Signature in itself has a mechanism to uniquely identify a business entity. The uniqueness of a business entity is typically established by validating against a 3rd party database the unique identifier issued by a National authority (e.g.) agency for business registration and tax authority. By definition, the reference database is available only for National enterprises.

B. Bid Encryption

17. The accumulated value of tenders processed using an e-GP system is very high and usually in the range of hundreds of millions of USD. The minimum threshold of procurement covered under e-GPA for goods and services in USD 100,000 and for construction services is USD 4 Million. Given that competitive bidding is adopted and taking into account the transparency and secrecy principles underlying Government Procurement, it is essential that e-GP system is designed with adequate checks and balances to ensure secrecy of bids (i.e. especially commercial bids) submitted online.

18. There are two key methods to ensure secrecy of bids submitted online:

(i) Symmetric key encryption: The same cryptographic key is used to both encrypt and decrypt bids. It is not safe and trustworthy when encrypted cipher text and the key required for decrypting the same is stored in the e-GP system. In such an implementation, the e-GP implementation agency will have access to both the encrypted bid and the key required to decrypt the same. Thus, one could allege that e-GP implementation agency illegally viewed bid details uploaded by bidders online in e-GP system. Those who prescribe adoption of symmetric key encryption argue that audit trails built in the system will have trace of any unauthorized transactions. Also, adequate process controls are put in place to ensure that illegal actions do not take place in the system.

(ii) PKI based Asymmetric key encryption: PKI based encryption of bids provides a safe and trustworthy method for encrypting bids. Herein, bids are encrypted using public key of the Government official inviting tender. The private key – corresponding to the public key – required for decrypting bids is available only with the Government official. The bids cannot be decrypted without this private key. Further, controls built within the e-GP system will disallow government official from decrypting bids until certain conditions are met (e.g.) expiry of bid opening timeline. In asymmetric key encryption, one person cannot compromise confidentiality of bids by acting alone.

19. The adoption of asymmetric key encryption is not a barrier for international trade because only purchasing agency officials require Digital Encryption Certificate. Bid submission process from bidder's point of view will remain the same. Hence, Government agencies can choose to adopt e-Signature for authentication and digital encryption for bid encryption.

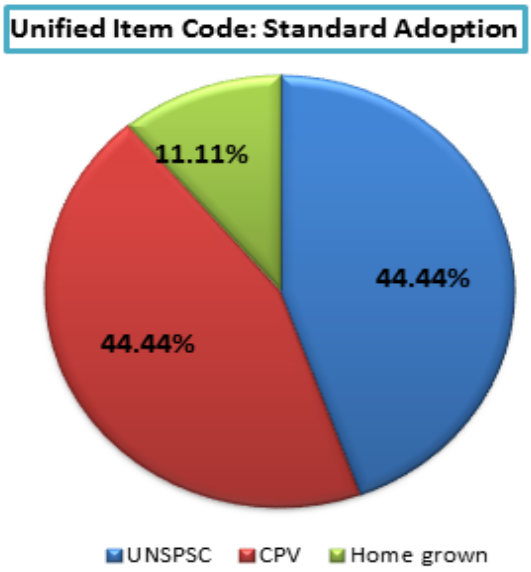
C. e-Payment of Bid Security

20. Business entities should have provision not only to submit their bids online using e-GP system but also the provision to transfer online bid security or any other bid submission related payments. In systems where such a provision is not available, business entities are typically asked to upload during online bid submission scanned copy of Bank guarantee or other payment details. Bidders will then have to submit the original financial instrument to purchasing entity within the date and time prescribed in tender document. In e-GP systems where manual submission of financial instrument is sought, transparency and ease of use associated with e-Bidding is adversely impacted.

21. Certain systems require bidders to compulsorily pay bid security and other bid submission payments online using e-Payment options integrated with e-GP system. Few of the e-Payment options might require bidders to have pre-existing banking relations with National Banks. For example, bidders shall submit Bank guarantee from only one of the National Banks which are connected with e-GP system. Such a requirement will create hurdles or even disallow foreign bidders from participating in tenders.

D. Consolidated View of Government Business Opportunities

22. Government business opportunities are now advertised online in e-GP system. Though the practice of advertising in paper media such as newspapers and trade journals continue to exist, business entities will find it easier to learn about business opportunities online. The European Union for example has developed Tenders Electronic Daily (TED) as a unified tender information portal wherein information about Government procurement contracts from EU Member States is advertised online.



23. EU has adopted Common Procurement Vocabulary (CPV) as the standard for categorization of tenders. As per a survey of 29 Asia Pacific countries conducted by Asian Development Bank in 2014, two codification standards viz. CPV and UNSPSC are being adopted. Refer below for a pictorial view of the study findings.

24. The World Trade Organization (WTO) uses multiple nomenclatures to codify Government Procurement viz. Federal Supply Code, Combine Nomenclature, Harmonized System, Customs Cooperation Council Nomenclature, Services Sectoral Class List and Provisional Central Product Classification. These codification mechanisms do not correlate precisely with CPV and UNSPSC.

III. CHALLENGES AND WAY FORWARD

A. Standardized Implementation of e-Authentication in e-GP systems

25. Currently, there are a large number of variations in e-Authentication implementation in e-GP systems. Business entities especially find it difficult to use e-GP systems which require digital signature based authentication. Just as EU enacted a Law to mutually accept digital signatures issued in its member countries, it is likely that many more countries will work together to mutually accept digital signatures issued in foreign countries as valid. Thus, the barriers created by digital signature in international trade will get reduced somewhat in future.

26. Meanwhile, an effort needs to be made to develop an e-GP specific reference guide that defined in detail the implementation approach to be followed for authenticating user identity and attributing action taken in e-GP system to a user. Specifically, this guide should detail the procedure to operationalize reliable implementation of e-Signature as defined in Article 6 (3) of MLES. Then, an attempt should be made to convince the e-GP system owners with digital signature based authentication to at least provide e-Signature (as defined in the reference guide) as an optional authentication feature for transactions open for international bidding. Authentication framework in which case becomes a configurable feature and NOT “one size fits all”.

B. Unique Identification of Business Enterprises outside National Boundaries

27. e-GP systems are increasingly integrated with 3rd party IT systems to validate identity of business entity and to uniquely identify a business entity in their system. Such identification however is limited to National businesses as on date. The e-GP systems in general allow international bidders to register online without any validation because as on date there is not a mechanism to reliably verify identity of business entity outside national boundaries. This lack of validation is a loophole in the system which some user could potentially exploit to obtain multiple user identities in the System.

28. An effort needs to be made to develop a mechanism to reliably validate identity of business entities internationally.

C. e-Payment of Bid Security across International Borders

29. e-Payment of small value payment usually does not pose a challenge due to the global presence of credit card companies. Not all e-Bidding payments are of small value. The value of bid security for tenders open for international bidding will be significantly high and it has to be paid using Bank guarantees. A few e-GP systems have made provision for National Banks to authenticate their identity and upload Bank guarantees issued by them. This provision will not work if an international bidder seeks to provide bank guarantee from a Bank in its home location. The banking mechanisms associated with international trade have to be thoroughly studied to evaluate if there is a mechanism to allow bidders to transmit Bank guarantee details online to e-GP system regardless of whether or not the issuing bank has any partners in the country hosting e-GP system.

D. Global Portal on International Government Business Opportunities

30. The enabling provisions for international trade such as the GPA will result in cross border trade only when business entities learn about business opportunities advertised

elsewhere in the World. It is cumbersome for business entities to visit multiple e-GP sites across the World to find out if there are any business opportunities suiting their line of work. Ideally, all relevant business opportunities should be consolidated in a single unified web-portal just as in TED. The development of this Global portal will catalyse international trade in Government procurement segment. Further, there is need to evolve a unified global standard for codification of government business opportunities. Business entities will find it easier to identify business opportunities in their line of work when a unified global codification standard is followed.