# E-PROCUREMENT-SECURETY ISSUES

4.1 The World Wide Web is changing the way the world engages in business. E-commerce/e-procurement consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. With this paradigm shift comes uncertainty about how secure e-commerce/e-procurement transactions are over an inherently insecure medium-the Internet. Like a chain, the security of e-commerce is only as strong as its weakest link. The arrival of ecommerce has created a whole new generation of problems - most surrounding the issue of security. The ecommerce security issue is, however, one that can be tackled... but only through a combination of measures. Effective management of ecommerce security requires deployment of a number of types of control. These controls are armory against intrusion and attack. They are the defense to any organization and its information assets. It is important, therefore, that we should address the issues carefully, and select the right tools for the job and employ them diligently.

4.2 Why be secure? Information is an asset, and like other important business assets it has value to an organisation and could be of value to competitors. It must therefore be suitably protected. Connecting computers to the Internet allows consumers and businesses to access a wealth of information and resources. However, it also creates the risk that computers may be tampered with by hackers, or attacked by viruses distributed via email. It is important to protect computers and information assets against these risks.

4.3 Consider these points:

- Initially, security adds to the cost of doing business. However, in the long-term it could save money, reputation and customers.
- Security is a process, not a project or a product.
- Continuous improvement is the key success factor for a good security program.
- Building and maintaining trust and credibility with customers and business partners is critical to the success of business.

**Security and Encryption Issues**

4.4 One of the issues most often cited by procurement specialists as a significant concern in shifting to an internet-based form of procurement is that of security. There are two broad areas of concern. First, the internet itself is, by its nature, inherently insecure. Second, to be effective and e-procurement initiative requires the exchange of often mission-critical (and therefore very revealing) data between buyers and sellers. For most organizations, procurement-related data-financial data, pricing models, strategic plans, expected new product announcements-can easily be used by competitors to understand company positioning and strategy. Again, there are two key issues to address. First, what information is to be shared? Second, with which partners in the supply chain should it be shared?

4.5 In many ways, technology is not the issue, however, because there are (or soon will be) any number of reliable techniques for maintaining the secrecy of data online. Solutions to technical security issues are already coming onto the market. In this regard, Digital Certificate Technology is becoming pivotal to the success of e-procurement, because it promises to provide reliable and verifiable identification of online partners. At the heart of the technology is a digital signature, which is based on public key cryptography and makes the electronic transaction legally admissible. Much likes an ATM card, which has both a public code and a private PIN, digital signatures identify parties through an independent third-party verification group, and the transaction is electronically validated so that it cannot later be denied. This "undeniability", or "nonrepudiation", becomes critical to procurement transactions.

4.6 Another good example of fast evolving security solutions is public key infrastructure (PKI) technology, which is being use on commercial online purchasing and smart card transactions. The program, known as ACES (Access Certificates for Electronic Services), issues digital certificates in real time and online, so that parties conducting business with the government can be identified while engaged on the internet. These electronic certificates provide government procurement officers with a means of authenticating the identity of the other parties before they begin confidential discussions. These digital certificates will form the basis of real-time, all electronic government procurement, where no other signature or authorization is required.

4.7 In fact, the government is spearheading many of these efforts. They have another program that is similarly based on digital certificates, but also combines the use of smart cards-much like standard procurement cards, in that they contain a powerful computer chip embedded in the card so that they can store critical data that ranges from identification codes to transaction data. And apart from using smart cards and PKI technology themselves, many governments are already debating legislation that will make these types of "electronic signatures" legally binding. It is only a mater of time before other technologies-fingerprint or retina scan techniques-become the norm.

4.8 Still as a recent survey of European procurement specialists reveals, a hesitancy to complete sensitive procurement transactions online is more often a question of cultural mindset than of practical encryption techniques. In fact, in a Price Waterhouse Coopers survey of 400 senior business leaders in the UK, Germany, France, and the Netherlands, trust and security issues were named as the two most important factors that were holding back e-procurement progress. It proves how old habits die hard. Nearly two thirds of respondents said that they sought a "trusted relationship" with vendors before they began to deal with them electronically, and nearly as many 60% -preferred dealing with bricks-and-mortar companies over Internet-only suppliers. Oddly, though, very few of the companies, even those more advanced in the use of e-procurement, had implemented the security systems available to ensure security. The same report concluded that almost two-thirds of companies relied only on standard password protection when dealing with suppliers over the internet.

4.9 And, of course, security concerns are not limited to the buying company of alone. Transparency of data on inventories, price, and performance means that suppliers too are feeling exposed. This type of honesty and transparency may well undermine a supplier's ability to manoeuvre, as buyers quickly learn to calculate a vendor's costs, profit margins, and stock (and therefore, desperation) levels.

4.10 In many ways, thought, procurement specialists are talking more about trust issues than technical security. With more and more information being shared between buyers and sellers, a new level of trust becomes necessary-one that pointedly may not exist within the sterile online e-markets, auctions, and exchanges. ORM is one thing, but reliability is everything in purchasing direct material issues of dependability, liability, and security are uppermost in the minds of those procuring direct materials.

4.11 All of this again highlights the need, particularly with the procurement of direct goods, for closer buyer-seller relationships than those found through e-markets or online exchanges. Today, suppliers not only need to be dependable, with reasonable price offerings, but in order to participate in the new world of e-procurement, they increasingly are being expected to have the ability to integrate their technical infrastructures closely with the buyer's technical infrastructure and to be able to change their business processes to adhere to the buyer's wish for end-to-end automation. They are also expected to absorb a good deal of the liability, through service level agreements. In the near future, companies will need to move more and more toward collaborative product design and sharing long term forecasting with their most trusted suppliers.

## TRUSTING THE INTERNET

### How to choose the best authentication system?

4.12 When authenticating the identity of staff within an organisation or visitors to a website, businesses face a number of choices. The table below summarises the main options available, how they works and their pros and cons.

| Technology | How it works | Pros | Cons |
|---|---|---|---|
| **Password authentication** | Matches user name and password to restrict access and authenticate identity | • Inexpensive<br>• Well understood by users<br>• Can be readily | • Can be compromised by users<br>• Does not authenticate data<br>• Often transmitted |

|  |  |  |  |
|---|---|---|---|
|  |  | changed | insecurely |
| **SSL (Secure Sockets Layer)** | Creates a secure connection between Internet application and user | • Widely supported in Web browsers<br>• Offers protection for all data transmitted between servers | • Customers cannot choose when it is used<br>• Relies on passwords for initial access |
| **PGP (Pretty Good Privacy)** | Uses public key cryptography; keys can be generated and authenticated by individual users | • Keys provide higher levels of authentication<br>• Supported by many software packages<br>• Cannot be easily changed | • Private keys can be compromised<br>• Public keys required to send information |
| **PKI (Public Key Infrastructure)** | Uses public key cryptography; keys are generated by certificate authorities | • Keys provide higher levels of authentication<br>• Used by governments and major companies<br>• Cannot be easily changed<br>• May be used with biometrics to access private keys | • Issuing certificates can be costly<br>• Businesses may require multiple certificates<br>• Private keys can be compromised<br>• Public keys required to send information |
| **VPNs (Virtual Private Networks)** | Create encrypted 'tunnels' between corporate networks and the Internet | • Give easy access to remote users<br>• Can | • Expensive to implement<br>• Does not support transactions |

| | | | |
|---|---|---|---|
| | | provide sophisticated access controls | with consumers |

## How to make sure our digital certificates and keys are secure?

4.13 To ensure the security of online transactions, many companies make use of public key cryptography, which uses digital certificates and a pair of unique 'keys' to identify a business or individual involved in a transaction. Digital certificates and keys provide a strong degree of security for electronic business. However, as with any security device, they can be compromised if not protected properly. When using digital certificates, a major concern is to make sure that only the person or business they identify can access and use them. For instance, if the key issued to a user is simply stored as part of their email program, anyone with access to their personal computer (PC) will be able to send or tamper with emails. If the machine is connected to the Internet, this might happen even if someone doesn't have physical access to the machine.

4.14 A basic method of protecting stored keys is to assign them with a password. When a user wants to sign a message, they enter the password to make the key available. However, a skilled hacker might be still able to read the key from the PC without knowing the password. A more secure method of protecting a private key or certificate is to lock it into an electronic smart card, which can be accessed on a PC via a smart card reader. A smart card is usually password-protected as well, so that simply having possession of the card does not enable anyone to use it. This is a more costly solution, as it needs a smart card reader added to the PC. A similar approach uses a hardware 'token' which plugs into the USB

(Universal Serial Bus) port which found on most modern PCs. These tokens are compact, and can often fit on a key ring. Because most new PCs have a USB port, they also don't need a separate reader.

**How to manage our e-security when the service is outsourced?**

4.15 Many small businesses choose to outsource their information technology requirements so they can concentrate on their main business objectives. This approach can be successfully extended to e-security, especially if an outside company is used to host your business website. Outsourced e-security services are often referred to as secures managed services, and is usually provided for a fixed monthly fee. Secure managed services can also be an effective way of implementing technologies such as firewalls and anti-virus packages. The main benefit of secure managed services is that small- and medium-sized companies do not need to invest heavily in e-security technologies or training. However, the business is still responsible for ensuring e-security is adequate. Any arrangement with a secure managed services provider should be based on a well-developed Service Level Agreement (SLA) that outlines the quality and type of service required and includes penalties for failure to deliver.

**How do we tell if we are completing a secure transaction?**

4.16 When conducting transactions online, it is important to make sure they are carried out securely. The most common mechanism for ensuring secure transactions on websites is Secure Sockets Layer (SSL). SSL is widely used because it is supported in all the major web browsing software packages. To ensure that a website that is selling a product or service is using SSL, look for the small padlock in the bottom right hand corner of the Internet browser. When the padlock in the bottom right hand corner of the Internet browser appears on the screen, the computer has successfully established a secure connection with the website. This ensures that personal details, order details, credit card details, delivery address and contact telephone numbers are protected whilst they are sent to the online store. Apart from the padlock, using SSL is virtually an invisible process. We will also notice that most sites using SSL have an address that begins with https:// rather than http://.

## CONCLUSION

4.17 ICAR should evolve an internal policy for overall IT/business security in consultation with IT security experts of NIC and CERT-IN of DIT. The policies must be clear, concise and effectively cover all relevant security issues. Once the security policy is implemented, it needs to become an integral part of day-to-day business activities and general business culture. ICAR should also review security policies on a regular basis, and discuss any concerns. Staff education is also important. Staff needs to keep abreast of information on current Internet security issues so that the security policy develop stays up-to-date. No matter how effective the service provided to us, it can be compromised if staff are not aware of security policies on issues such as creating and protecting passwords, sending email securely and carrying out transactions online. Another important step to be taken is to procurement of Security software tools such as IDS, timely up dation of anti-virus software. ICAR should making use of DR centre of NIC for keeping the back up of critical data of e-Procurement application once it is launched.