Odyssey Technologies Limited

CIN: L51909TN1990PLC019007

INVESTOR FAQs

September 2015

PREAMBLE

From time to time, we get questions from our investors about the various aspects of Odyssey's business. Though we are not in a position to offer financial guidance at this time we felt that it is our duty to answer these questions. As we do not follow the practice of meeting one-on-one with any investor/analyst to discuss the state of Odyssey's business, all such questions are aggregated and answered to the best of our ability without breaching customer confidentiality or exposing competitive information.

DISCLAIMER

Certain statements made in this FAQ concerning our future growth prospects and/or any forward looking statements contained herein are based on assumptions and expectations that we believe are reasonable as of this date. Forward looking statements/ assumptions regarding growth prospects by their nature involve a number of risks and uncertainties that could cause actual results to differ materially from market expectations. This FAQ represents only the Company's current intentions, beliefs or expectations and the company assumes no obligation to revise or update any forward looking statements as such.

Odyssey Technologies Limited

CIN: L51909TN1990PLC019007

INVESTOR FAQs

I.Technology and Products

1. How difficult was it for the company to keep focus on its area of developing a product in public key infrastructure (PKI) technology while most of the other information technology (IT) companies focussing on services and other technologies were growing rapidly? Did the management consider entering into a new technology or segment while it was going through the tough times?

   The company has maintained its focus on product development all through and was structured to facilitate that. IT services are a different kind of business altogether calling for different competencies at every aspect like sales, project management and development. The people management approach for services also has to be different. Managing both a service arm and a technology/product arm simultaneously is possible only at a much larger scale like SAP / Oracle / Microsoft. There are few companies worldwide which have managed such a feat and attempting that at the stage Odyssey was in during those years would have entailed existential risks for the company.

   Admittedly, certain other technologies have grown more rapidly during the period. At the same time, a fair amount of technologies have dwindled and died during that period. The choosing of a technology and investment there in always has inherent risks and to succeed, an organization has to maintain focus during the various vicissitudes and not hop from one technology to the other at the first sight of trouble. Whether the chosen focus bears fruit or not, frequent changing of it will certainly not.

2. Our understanding is that the one important feature of PKI technology is "non-repudiation" which is not present in most of the other competing technology. How important is "non-repudiation" in PKI gaining momentum for transaction based services (e.g. tax filing/online banking/e-commerce)?

   Yes. Non-repudiation is a feature of PKI technology which is not present in any other competing technology. It even has the legislative blessing. But in our opinion, it is unfortunate that this aspect got highlighted out of all proportions.

   Non-repudiation is a great feature to have if your current security problem is primarily 'repudiation'. If a large number of customers get into the habit of doing transactions and later disputing them, then non-repudiation helps. Yes. Some time repudiations of genuinely carried out transactions do happen but they are too few and too far between to worry anyone. Most of the times, when a customer claims that he had not done it, it turns out that he really did not do it and someone compromised his account. We generally do not get to hear someone issuing a cheque and then later claiming it is a forgery. We do not hear of customers doing credit card transactions

and later disputing. If a customer disputes that he did a transaction, nine out of ten times he really would not have done it.

People repudiate their actions only when they know their actions to be shameful or a crime. Most people would deny that they visited a pornographic web site, and drank liquor when prohibition is in force. That is where some kind of non-repudiation can help. But obviously people are not going to be using PKI when they are committing a crime or transgression! So either way, it is no good. Genuine customers will look at the suggestion of non-repudiation as an insult to them and fraudsters are certainly not going to be signing their fraudulent transactions with their digital certificates.

Then of what use is PKI? PKI is the only technology that can offer end-user protection and security and leave the power to compromise his accounts only to himself and no one else. We keep hearing of hackers stealing millions of credit card numbers and passwords every day. Every one of these successful heists is putting a large number of customer accounts at risk – either financially or when it comes to health care, risk of losing privacy.

This cannot happen with PKI. We don't ever hear of a hacker stealing digital certificates! Because digital certificates are public documents and stealing them would do no good or harm to anybody. The security of PKI rests with the individual user's private key which is always in his care. Even in other seemingly secure methods like one time passwords, the service provider and possibly the vendor of the solution, have a copy of the customer's seeds. And these seeds could be stolen. Insiders can compromise the seeds and put customers at risk. Mobile OTPs can be stolen by Trojans before the recipient sees it. Elders and the less informed can be fooled into giving away their One Time Passwords by Vishers. But no one can fool you into giving away your private key because you do not have the ability to share it digitally. The only way to compromise a PKI user is physically robbing him of his private key token. No one can compromise a service provider like a bank and thereby making the bank's customers collateral damage.

If we look at it properly, this is actually the converse of non-repudiation. Here if a customer sees that a transaction is attributed to him, he can challenge the service provider to show him his digital signature for that transaction. There is no way someone can forge his digital signature and therefore the customers' duty of repudiating the transactions they did not do becomes much easier in PKI. In other systems it is very hard and a large number of records have to be examined and circumstantial evidence brought in, before a tribunal or ombudsman will determine that the customer did not do the transaction.

It is only when this knowledge becomes commonplace, PKI will have really arrived.

3. Odyssey has a range of product offerings in below area
    o Transaction authentication (Snorkel)
    o Certificate management solutions (Cetrix)
    o Electronic document distribution (Alta Signa)
    o Mobile data collection (Epic)

Help us understand the target customer group for each of this product group and how they rank in revenue generation and scalability. Also explain to us about the stream of revenue generation – product license, product related services etc. and the brief terms of product license and product related services. Does product related service mean that it is recurring in nature?

We would prefer not to talk about individual product related revenues other than what we have already disclosed in our Annual Reports due to various customer sensitivities and competition intelligence.

Product licenses are generally sold one time and sometimes result in repeat license revenue when a customer expands the scale of the product deployment.

Product related services include Pay-As-You-Go charges, product implementation, annual maintenance, occasional customization and on-site support if desired by the customer.

The various numbers constituting these have already been presented in our Annual Report and the Management Analysis there.

4. It appears that the company has sought to move to "pay-as-you go" model from earlier model of one time/recurring fixed license fees. How does this business model work? Is the "pay-as-you-go" model currently adopted across all product groups or is it specific for some of the product groups? What are the advantages and disadvantages of "pay-as-you-go" model as compared to fixed one time/recurring license fee model? Is the "pay-as-you-go" model dependent on number of transactions or the transaction amount?

We have made the PAYG model available across the products. The customer choice of this model over outright license purchase varies depending on the customer and his needs.

Both the models yield more or less the same revenue benefits to us. As such, it really does not make a serious difference.

But for the customer, there are quite a few differences. PAYG allows the customer to seamlessly scale up his usage and incurring expenditure only when he really uses it, avoiding a larger initial outlay. Further, he incurs the entire expenditure as revenue

expenditure. On the other hand, outright licensing requires a capital expenditure but at the same time the overall cost is estimated up-front – which is important in the case of Government purchases and large organizations where the needs for fixing budget approvals score over the advantages of PAYG.

5. Even though, PKI is one of the preferred technologies for digital transactions, there exists a technology obsolescence risk. How large the impact of this risk can be on Odyssey and what is the likelihood of this risk materializing? Do we have an alternate plan in terms of such risk materializing?

   In our opinion, PKI faces the least technology obsolescence risk. Such a risk can come about only by the basic tenets of Asymmetric Cryptography (which is the basis for PKI) failing – like someone managing to break the algorithm itself. In the current state of technology, that would not happen for quite some time to come.

   The real risk comes from less-secure, more user-friendly and flashy technologies sidelining PKI. In our experience this happens with almost predictable regularity and such temporary mania dies down after a while, leaving PKI again as the more reliable option.

   ## II.Industry

6. We understand that digital security involves very broad expanse of activities and technologies, however it will be useful if you can throw some light on the size of the industry as whole in India. As sub segment of this market, what is the size of PKI based security market in the country? What are other prevalent major technologies in the space in India?

   No comprehensive details are available about the overall size of the information security market in India. The estimates of Industry Analysts vary widely ranging between 150 million to 1.2 billion USD. This is because no established definition exists about what rightly constitutes information security. Depending on the purpose at hand, analysts club everything from security camera systems in public places to highly specialized cryptographic software, covering along the way firewalls, intrusion detection systems, virus scanners, anti-spam software etc.,

   Considering the omnibus nature of the industry, our concern should be only on those technologies that actually serve as alternatives to the ones the company is offering, primarily in the authentication space. Again, it is difficult to guess the total size of this market because the current methods of authentication vary widely from very weak, automatic authentication mechanisms to passwords to biometrics to PKI and a whole host of others in between. In several situations, a default authentication mechanism provided by the application itself is considered adequate by the service providers. Our best guess at this point would be that the overall authentication market may be

of 40-50 million USD. We should bear in mind that this is a very volatile number and keeps changing on the basis of technological and business evolution.

7. Considering the tail winds of regulatory push for PKI adoption, increased awareness about security threats amongst stakeholders and increasing digitization of services, how do you see the industry as a whole growing in medium to long term?

The regulatory push certainly helps. But except for government applications, most other transaction applications have only a mandate to offer PKI as one of the alternatives. While this does help in a large number of digital certificates being sold and PKI based authentication mechanisms being deployed, the real market growth will happen only when some form of PKI becomes the preferred choice of the customers.

Even with the increased threat profiles and increasing digitization, the end-customer craving and adoption only can drive this in the long term.

8. OTL has been working on for last 3-4 years to tap two large opportunities emerging in digital world i.e. mobile transactions and cloud computing. However, latest annual reports suggest that
   - The security solutions market for "mobile transactions" are still some time away
   - Specific niches within cloud computing offer room for specialized security products

What are your views on the scale of monetization of such opportunity and the time-frame involved in monetizing these opportunities?

We have been reengineering our technology/products to fit the mobile transaction segment and also to work at the scale this segment requires. We are confident that these efforts could be monetized over the next 2-3 years.

We are not as confident any more about the opportunity in cloud computing security and we have scaled down our efforts there. We will be ready to take a relook at that segment if things change.

9. RBI has come out with draft guidelines in February 2014 asking the banks to implement the guidelines in phase wise manner from 6-18 months for corporate banking and retail banking. What impact do you envisage because of these guidelines on Odyssey's business?

As stated in an earlier answer, the guidelines will ensure that PKI based transaction authentication systems are deployed in almost all the banks. But in the absence of any indications as to the end-user adoption, most banks will resort to PKI implementation with a minimal capacity of users initially. Therefore, the revenue

impact from the guidelines will not be huge for now. The real impact will be felt only in the next two to three years or more.

10. There is lot of talk on cyber security in present world and there are various companies working in this particular area. Is our company trying to pitch into Cyber security -If yes, on its own or through a partner?

Cyber security includes a wide gamut of hardware, software and predominantly services. For instance the large majority of what goes under the label are Firewalls and other perimeter devices, virus scanners, Intrusion Detection Systems etc., Lately even the video monitoring systems and other sensor networks are clubbed under the umbrella of cyber security. PKI and other high-end authentications systems form a part of this larger framework. At the moment we are not planning on entering these other areas of cyber security as we foresee sufficient opportunities in our areas of expertise.

III. Market segments

11. We understand that as of now, four major users of PKI based technology in the country are

   1. BFSI   2. Defence   3. Healthcare   4. Government

   How is the overall PKI solution market divided amongst these four major users of PKI technology? Is there any other industry where there is likely to be reasonably large opportunity for adoption of PKI technology?

   Currently in terms of volume it is almost evenly divided between Government and BFSI with Defence and Healthcare constituting marginal adoption.

   We believe that all other industries will trail BFSI and seek to ride on the infrastructure stimulated by BFSI.

12. We see that we have also entered defence PSUs . What is the size of the market for security products & services offered by us in defence area which is right now considered to be a hot business segment and what is going to be our strategy for growth.

   For now, the business with defence PSUs is much smaller than the BFSI segment. Even for future, we believe BFSI and eCommerce would be the biggest consumers of PKI and therefore a majority of our efforts are focused there.

13. Apart from banking, healthcare is gradually becoming a big market segment. What kind of opportunities we are looking in this area? Also equally important segments are online retail and education - What is the perception of management in terms of business opportunities from the above sectors?

Again, healthcare can be a huge growth area but right now it is still getting its act together. There is nothing comparable to Core Banking or Internet Banking there that will enable marshalling of data and access through well-defined, standardized channels where it can be effectively secured. We will be able to see revenue there only when that happens.

14. Do we see opportunities for our products and services in export market?

Yes.

15. A product Company needs strong marketing muscle. Hence we need huge capital to penetrate domestic and international markets and also for recruiting and retaining skilled human resource. How does our management intend to address this particular issue?

PKI does not demand widespread marketing efforts unless we are offering end-user devices and software directly to end-users. We are deploying our products primarily for the service providers and therefore only focused marketing helps here. This may change in the future if and when we offer any product in the end-user space.

We do have a small sales team complemented by our partners' sales efforts. We are in the process of ramping up the sales team.

We are still working on our international market strategy and the answer to this question will depend on how the strategy evolves.

16. As the Company has been making profits in the recent years we hope that the Company will put in place a suitable policy for distribution of profits to shareholders and at the same time will bring a stock option policy for retaining and rewarding its employees. Also it is desired that suitable policy needs to be implemented for Corporate communications since the stock has started getting attention of retail and HNI investors.

The company still has to recover its losses fully. We would certainly work on these policies and keep our shareholders informed of any significant development in this area.

We will certainly seek to improve our communications with investors as a whole. At this juncture we find it difficult to offer one-on-one meetings to our investors and choose to address the entire stakeholder community as a whole.

17. Over last many years, through ARs, the company has indicated that the largest opportunity for the company remains internet transaction authentication solutions market which we understand is addressed through Snorkel product groups.

However, what we have observed is the in terms of contribution to the overall revenue, Snorkel's contribution has come down from more than 70% to less than 40%. On the other hand, the contribution from Certix has consistently improved from 8% to 37%. What may be the underlying factors for such disconnect?

There is no disconnect here. Our authentication products rely primarily on digital certificates. As such, the certificate issuance has to happen before the certificates can be used in other applications. The advantage of PKI over other technologies is that a single credential like a digital certificate can be used by the end-users to access several separate web resources, be they banking systems, trading systems or compliance interfaces. This is in contrast to the various password and One Time Password based systems where each service provider has to maintain independent systems for credential management and the end users are burdened with multiple credentials, one for each service. Once a digital certificate is issued, perhaps to be consumed by a single authentication or compliance system, other services can ride on the same certificate. Thus the nature of the model dictates that the issuance systems will grow first followed by the authentication systems and in fact, that is what is seen here.

18. R&D and product development continues to be one of the largest expenditure for the company, constituting more than 50% of company's revenue. What are the typical steps, cost and time frame involved in new product development? Is there any established matrix to evaluate the viability/attractiveness of new product development before the company decides to make investment? How difficult was it for management to keep spending money on R&D while it was incurring loss?

All R & D does not relate to only new product development. PKI being governed by a compendium of standards and individual regulatory environments, evolution of these environments force product vendors like us to continue to invest in R & D work to ensure our products continue to work and satisfy the changed stipulations. Further, our products predominantly work in the web environment and are heavily dependent on the various browsers and similar mechanisms the end-users use to access the web based services. The more popular browsers are in a continuous state of flux owing to their perceived competitive advantages, changes in standards like HTML, CSS and scripts, enhancements and changes to transports like SSL/TLs etc., After

all these, the changing threat profiles in the Internet also have to be monitored continuously and the products need to react to the changes therein. Most of these changes are non-trivial and cannot be dealt with a simple customization of the product. Continuous R & D is the only answer there.

Having said that, we also engage in new product development in equal measure. Generally, a product decision is taken on the basis of a fundamental change in technology that creates a product opportunity or a new regulatory requirement that creates a product niche. Even there, we generally prefer to acquire at least one customer for the proposed product before we invest significant efforts into the product.

A simple answer to the last part of the question is 'very'. We are happy to have crossed that bridge.

19. Customers are moving towards Apps for their banking & ecommerce transactions. Will the company be negatively affected?

Movement towards smart phones and apps has actually the effect of significantly expanding the market. Even with the large mobile wielding population, PC based internet access to these services is still expanding.

The Company considers this as an opportunity rather than a threat. We are working on addressing these markets effectively using our experience and expertise in authentication solutions. We expect these efforts to have a positive impact going forward.

20. What is the impact of traditional banking customers moving away from local banks to Paytm, Alipay, Paypal, M-pesa and the like?

Again, these new payment providers only expand the customer base and overall market size rather than taking it away from traditional banking. Further, the proliferation of payment services will reach some kind of equilibrium soon and then these will also become opportunities for security.

21. Banks are the company's primary customers. Once most of banks are covered with a security product, where will further growth come from?

Security needs to constantly evolve. We do not see the possibility of a panacea for all security needs that will saturate the market and inhibit further growth.

Moreover, as PKI based authentication takes hold in the banking segment, other industry segments also will become fairly active. The company's products are

engineered to be segment-agnostic and we foresee no problem in scaling in emerging areas.

22. Based on our understanding of the business, we feel that as the company's products gain more acceptance and the incremental revenue shift to pay-as-you-go model, the benefit of operating leverage will play out in future. Can you please help us understand at what level of business maturity/penetration/revenue are required to gain significant advantage of operating leverage start accruing to the company?

While we offer pay-as-you-go model on almost all of our products, the customer acceptance of the model is not as wholesome as we expected it to be. There are several factors at play here, predominant among them the reluctance of large organizations to commit to an open ended expense budget. They generally prefer to have a definitive number to facilitate their internal approvals. Therefore pay-as-you-go will confer significant advantage only when a large number of individual customers are involved. We see both models co-existing for some time to come. However, when PKI becomes the preferred transaction authentication mechanism, PAYG model may see a significant upside.

23. Is the Company's revenue coming from one-time product sales or is there possibility of annually recurring income from any kind of maintenance or service fees? Will revenue come from regular upgrades to existing products too?

As mentioned earlier, the revenue comes from both one-time license sales and annuities in the form of pay-as-you go revenues. These are complemented by Annual Maintenance Contracts in the case of license fees and upgrades to existing products.

Routine upgrades to existing products are generally covered under the AMC. But upgrades driven by specific customer needs also generate revenue.

IV. Operations and performance

24. The company had significant sales during the years 2000-2001. Thereafter the sales continuously declined and the company incurred losses during the period FY2002 to FY2008. Can you tell us why this was so.

In the year 2001, the sales figures included the transfer of a product to the company's wholly owned subsidiary. The amount of security product sale included therein was insignificant as the technology and products were at alpha stage at that time. The company incurred losses for the following few years as the security products were in the process of development and were yet to find market acceptance.

25. One of the major cost for the company is employee and manpower cost. This cost has increased significantly from 30% of revenue in 2009 to 50% of the revenue in 2014. What is the anticipated trajectory for this cost component in medium to long term?

The employee and manpower cost will continue to be a significant factor for an enterprise like ours, where the intellectual inputs are the primary raw material. That said we do expect the revenue to outpace the cost and this proportion to stabilize and then to come back to its earlier proportion of 30-40%

26. How does the company secure new customers? Does it participate in the tenders/RFPs floated by the customers?

Yes. This is complemented by our direct sales force as well as the partners who bring in both participation in contracts as well as their direct sales.

27. There has been significant addition to our client base during FY13 and FY14. Was it primarily because of the guidelines by RBI? Kindly highlight the impact of such a sharp jump in client addition to our revenues in medium term.

A need for a purpose-specific digital signature product arose during FY13-14 for participating in the NPCI's ACH system. This was a small product and since we had the technology we could build the required product in a very short time and offer it to a large number of banking customers, including co-operative banks. This had a small revenue impact not proportional to the number of customers. However, there is a large customer base out there now who know that we build standard-compliant, simple to use and resilient security products and we hope to leverage it when other opportunities in the space arise.

28. Even though, we have grown at reasonably good rate and are likely to reach Rs.10 Crore annual sales mark in near future, the size of the company still remains small compared to the size of the opportunity. As we have already successfully overcome the teething troubles and have come out of turbulent times, how do we plan to scale up from here on? What is your view on time frame required for Odyssey to reaching mile stone of 50 Crore sales and 100 crore sales?

We trust the mobile transaction security space will offer a significant opportunity for scaling in the near future. Technologically, we are in a state of readiness to exploit the opportunity when it happens.

However, we cannot put any specific number to the size of the opportunity and we would not like to make any kind of speculative statement here.

29. In your annual reports, you have consistently mentioned that we rely significantly on our partners to tap larger opportunities and they are important constituents in our growth strategy. Please elaborate how this partnership model works. What are the key roles/responsibilities of the partner? What are different partnership models prevalent (i.e. profit sharing/revenue sharing/sub-licensing etc)?

We generally do not enter into profit or revenue sharing models. Many of these opportunities usually have a significant hardware and implementation components which are not offered by us. We offer the software component to the partner who puts the entire solution together and implements for the customer. The product is billed to the partner at a transfer price.

30. Who are some of the major partners of Odyssey currently? Historically, what has been the percentage of sales coming through partners? Do we envisage any substantial change in this number (either positive/negative) in near to medium term on this front?

We have partnered with a few large System Integrators. Most of these partnerships are governed by non-disclosure agreements and we are not in a position to share the names.

The percentage of revenue derived from partner sales vary from year to year but it generally does not exceed 20%. We are working towards adding new partners and therefore we should expect this share to go up but it will do so gradually.

31. One of the aspects that Odyssey has consistently highlighted is that the partnership model restricts the flexibility of the company and impacts the margin adversely. It will be useful if you can put some broad numbers around the profitability of typical product with/without partnership. What kind of restrictions are placed on the company in partnership model (i.e. limited exclusivity, longer sub-licensing period at fixed cost, lower escalation etc)

We have only highlighted the fact that any increase in partnership sale would not yield the same margins as direct sales by us. However, we are also aware that the model is necessary to achieve scale going forward.

We have so far not sought or offered exclusivity to any partner.

32. As we have a reasonably good product portfolio addressing a large section of addressable opportunity in our field and our products have stabilized over last few years, the next focus shall be on selling the products to existing and new clients. How

are we planning to ramp up the sales and marketing function to take maximum advantage of wide ranging, mature and well accepted products?

We are constantly on the lookout for new partnership opportunities and we are also in the process of ramping up the sales team and coverage. We do expect that in the next two to three years, sales would form a significant portion of our total workforce.

33. In 2006, we had 64 employees on the rolls and in 2014, after going through a roller coaster ride, the head count in 2014 is 64. In contrast to that, the revenue has increased from 1.22 Crore to more than 7 Crore. We have mentioned in all annual reports that remuneration is equivalent to the best in the industry. In spite of that it is evident that scaling up an organization has been a challenge for us. In your opinion, what are the main contributing factors for such challenge? What steps have we taken/are taking to address this challenge?

Product engineering work is considerably more strenuous than carrying out customer specific IT projects. It also requires significantly more knowledge base, versatility and endurance on the part of the workforce. We consider our present workforce more or less adequate in terms of numbers for the product building activity. Further scaling up will be more focused on marketing, sales and delivery personnel.

In the past, the major challenge for scaling up in those directions was barely adequate cash flows and inadequate product maturity. We are now focusing on scaling. However, the growth in employee strength shall never be similar to IT Service companies where the revenue is directly linked to the number of people deployed.

34. What is the typical attrition rate at OTL? How does it compare with the peers?

It is between 20 to 25% which is a little higher than the industry average. Most of it happens within the first 2-3 years of employment. As said in the previous answer, product engineering can be quite draining and people do find that they are not temperamentally suitable for such work.

35. At what level of maturity do you see Odyssey's software development life cycle operating on CMM (capability maturity model) Level scale? In other words, how do we rate our software development lifecycle process on CMM level 1 to 5?

CMM is primarily meant for software projects. New product and technology development always has an element of controlled chaos about it. We would rather

measure ourselves on creative use of technology where we would place ourselves somewhere in midscale.

36. We understand that, Odyssey does not receive and store any sensitive data of the customers in their premise or control; however our products are essential in protecting these data. What kind of liabilities does company take in case of breach of security or unsatisfactory performance of its products? What are the risk-mitigation measures (i.e. insurance/overall cap on liability etc) that company takes in this regard?

   The overall liability is always capped at the total value of the project and this is covered by appropriate insurance policies.

37. One of the risks that the Company has mentioned in its AR is the lack of scale both operationally and financially that restricts it from participating in large opportunities. Help us understand the typical limiting conditions (i.e. minimum net worth requirement, minimum number of installations, number of banking clients etc…)

   Most of the time it is tied to historical revenue and sometimes to number of client installations. If we fall short, we do on the revenue front. Such opportunities are generally addressed through partnerships but there are occasional misses too.

38. Financial institutions are one of your biggest / most promising prospects. Have they expressed any reservations about buying products especially in the area of Payment Security from a relatively small entity like Odyssey? How is the Company addressing such concerns?

   Security being a technology intensive activity, companies specializing in that tend to be smaller in size as compared to large System Integrators and IT service providers. Most customers understand this and want the advantages of dealing directly with the experts in the area and do not mind the size. In fact most of the large banks in the country are our customers for one product or the other.

   We do not see real gains in permanent tie-ups with major names. From our past experience, such tie-ups end up restricting the specifics of what we offer and we do not see that as an advantage in the long term.

39. Does the results of last Q4 of 2014-15 signify likely poor performance in coming quarters, especially in terms of growth?

   We derive our revenue largely from product licenses and product usage charges. Some of these product sales happen in short engagements but many can take much

larger gestation periods to take shape. Therefore, it is difficult to predict or regulate the sales during any short time period like a quarter. The quarter on quarter performance will be relevant for IT Services, or for product companies like us, when we reach a really global scale.

V. Competition

40. In company's previous annual reports (2010-2012), it has been mentioned that company witnessed significant competitive pressure from global players through their local partners and system integrators. Has the competitive dynamics changed in last couple of years? At present, who are the major players in the PKI based solutions market in India? What will be the approximate market share of Odyssey in the overall market?

    Competition to PKI based solutions does not come only from PKI players but also from a host other technology vendors providing authentication solutions.

    If we look at only PKI based solutions, SmartTrust, an European vendor and Entrust, an European owned American provider do offer PKI applications and toolkits. Their toolkits are used by a few local players to offer their own solutions and these local players also resell some of their applications.

    Among Indian players, TCS offer their own PKI solutions too.

    Our estimate is that we are present in the PKI software solutions to the extent of about 25-30% overall. We should remember PKI solution offerings need a gamut of server, network and end user hardware components and at present we do not offer our own products for any of these needs.

41. Though we are growing, as compared to our competitors like Gemalto, TCS in domestic market we are much smaller. So what steps we are taking for withstanding such competition.

    Though the overall size of the company may be much larger in those cases, we are comparable in customer wins and revenue from PKI software space. We have managed to establish that we provide secure and compliant software solutions. Their overall size is larger because they cover a wider range of services and not just PKI.

42. In the annual reports from 2010-13, we have consistently mentioned about increasing competitive intensity and its impact on margins. Please help us understand the competitive intensity in the space. How high are the entry barriers for new entrants in the space considering the "cryptography" being a highly specialized technology?

Odyssey Technologies Limited

The entry barriers for building native applications is quite high in this space. PKI is a little complex in its underpinnings and complying to a plethora of standards and regulations and handling external dependencies is hard to get right and takes time.

However, the competition comes from vendors reselling a overseas PKI product or smaller products using development toolkits from established PKI vendors.

Another face of competition is from non-PKI security vendors competing with PKI. Frequently, those solutions are simpler and less expensive to deploy initially – but in the medium to long term PKI shows up better. Even so, these vendors do represent a significant competitive pressure.

******