WISeKey International Holding AG

Switzerland | Digital Security Technology

Initiation of Coverage

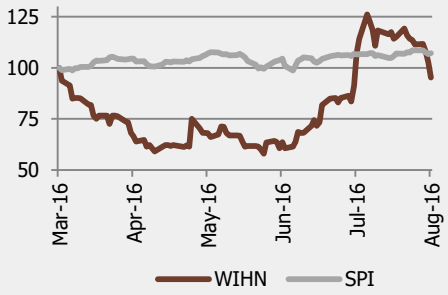
22 August 2016

Company Data

Price:	CHF5.33
Market Cap (incl. class B equivalent of class A shares):	CHF127m
Free Float (incl. class B equivalent of class A shares):	66.4%
Avg. traded vol.(since listing):	42'707
Bloomberg:	WIHN SW
Reuters:	WIHN.S
ISIN:	CH0314029270

Source: SIX Swiss Exchange and Bloomberg

Share Price Development *(rebased)*



Source: Bloomberg

Key Financial Data (CHFm)

	2014	2015	2016e	2017e
Sales	3.3	2.2	28.0	95.8
EBITDA%	NM	NM	(15.9%)	14.5%
EBIT %	NM	NM	(16.9%)	13.5%
Net Margin %	NM	NM	(16.6%)	14.0%
Net Income	(31.7)	(6.2)	(4.6)	13.4
Diluted EPS	(0.5)	(0.1)	(0.1)	0.4
Equity Ratio %	100.0%	100.0%	100.0%	100.0%
Capex	0.1	-	0.7	2.4
P/E	NM	NM	NM	36.1x
EV/EBITDA	NM	NM	NM	33.1x
EV/EBIT	NM	NM	NM	35.5x

Analysts

Doris Rudischhauser
dru@researchdynamics.ch
Alexandre Müller
amu@researchdynamics.ch
Tel: +41 43 268 3232

Monetizing on substantial opportunities

WISeKey International Holding AG (Company) is a Switzerland-based cybersecurity company which acts as a Trusted Vertical Cybersecurity Platform developing technologies such as Root of Trust (RoT) online security, mobile security and identity management solutions worldwide. The key to WISeKey's offerings is its neutral cryptographic RoT technology located in Switzerland for ensuring cybersecurity across various channels of communications federated into its vertical platform. WISeKey's RoT technology is embedded in more than 2.6 billion browsers, sensors, wearables, semiconductors and Internet of Things (IoT) devices.

- **Vertically Integrated Platform, potential operational synergies and domicile in a neutral location**

  WISeKey offers clients a vertically integrated digital identity platform interconnecting its cybersecurity offering and IoT ecosystem. In order to leverage the Vertical Integrated Platform, WISeKey announced the acquisition of VaultIC, the semiconductor company of French embedded software firm INSIDE Secure. These enhancements should bolster WISeKey's profile as a cybersecurity IoT security player, with the chip-to-root capability, providing a potentially unparalleled trusted and secure IoT ecosystem.

  WISeKey could also drive revenue growth by integrating its solutions with SAP's industry-leading solutions as announced by both companies, reinforcing the current cybersecurity of SAP HANA, and also via the signed partnerships with Microsoft on CityNext and MasterCard on authentication and payment for wearable devices. WISeKey could generate operational synergies from its expanded offerings and potentially increasing applications in a relatively nascent IoT market. Moreover, WISeKey claims to be the only player globally benefiting from a neutral cryptographic rootkey store outside the US and other potentially conflictive jurisdictions, which opens new client acquisition streams specially in what concern the IoT Market and Industrial Internet requiring large deployment of Digital Identities.

- **Buying growth and applications through acquisitions and partnerships**

  WISeKey has expanded its offerings and markets both by strategic alliances, organic growth and, recently, through acquisitions. The company intends to grow further through complementary acquisitions and/or partnerships. The company expects to complete the acquisition of VaultIC, the semiconductor assets of INSIDE Secure in September 2016. WISeKey also announced an intention to merge with Swiss company OpenLimit in July 2016. OpenLimit is listed on the German Stock Market and has a strong footprint in Germany as the provider of the German Governmental National Identity and IoT services. WISeKey also has contracts and agreements with global customers and strategic partners including MasterCard, CenturyLink, Bulgari, Hublot, Bancorp, Airtel, Microsoft, SAP and Samsung. Besides, WISeKey is diversifying across geographies in a bid to create new growth avenues.

- **High-growth target markets and expansion in the IoT space to drive future revenue growth**

  WISeKey's solutions target high-growth markets such as mobile payments & security, identity management and IoT. According to global market research firm IDC, the global IoT market is expected to grow to USD1.7tn by 2020 from USD655.8bn in 2014. It is also predicted that the number of connected devices will grow to 29.5 billion in 2020 from 10.3 billion in 2014. WISeKey has invested resources in IoT technology (including acquisitions) in the past which

should enable it to start fully monetizing them from now on. WISeKey is currently deploying large-scale IoT digital identities for watches and has a proven revenue model in this emerging space, which other competitors are still trying to monetize. This trusted technology integrates wearable technology with secure authentication and identification, in both physical and virtual environments, and empowers IoT and wearable devices to become secure transactional devices. It is estimated that the global wearable market will grow at an annual rate of 35% over the next five years.

- **Valuation**

  We think WISeKey will continue to remain a strategic niche consolidator in the IoT cybersecurity space (rather than become an M&A target itself) since its Articles contain provisions that could prevent or delay any potential bid. Accordingly, despite the flurry of deal activity in the IT security sector and WISeKey's niche offerings, we expect the company to command valuations lower than comparable deals. Moreover, the lack of visibility on margins exacerbates the need for a deep discount, in our view. Based on a terminal growth rate of 3.0%, we arrive at a valuation of CHF14.9 per share. We adopt a bullish stance on WISeKey as the stock offers significant upside potential from current levels.

TABLE OF CONTENTS

INVESTMENT HIGHLIGHTS

Vertically integration, potential synergies from expanded solutions and neutral domicile status

WISeKey offers niche solutions in the highly dynamic and competitive IT security solutions landscape. In the recent past, WISeKey has made some strategic acquisitions which have provided the company with an unparalleled vertically integrated digital identity, security and IoT ecosystem. We believe this competitive offering, along with its RoT, is a key differentiator for WISeKey, given its ability to generate cross-selling opportunities and generate growth from new client acquisitions. Post the acquisition of the Semiconductor company VaultIC of INSIDE Secure, WISeKey will continue offering chip-to-root technology (as it is the case already with Bulgari Intelligent watch and Hublot watches) as WISeKey and INSIDE Secure are already working together since 2014 thereby offering an integrated solution including chips, asymmetric digital authentication and identification as well as encryption solutions. Moreover, WISeKey offers solutions which can secure IoT Edge devices as its solutions can be integrated with industry-leading SAP's HANA platform. Since SAP's HANA platform has gained wide industry acceptance, we think that WISeKey could grow this revenue pie substantially.

The IoT security landscape is still evolving even as the IoT adoption is likely to pick up. We believe early movers in this space such as WISeKey stand to gain big, since RoT is required for secure communication over IoT. We opine WISeKey could likely generate operational synergies from cross-selling opportunities in the space through its expanded offerings by integrating chips (INSIDE Secure), SAP's HANA and other key technologies.

WISeKey's IoT RoT is the only RoT acting globally which is located outside a NATO (The North Atlantic Treaty Organization) member country i.e. in Switzerland, thereby ensuring geopolitical neutrality and data sovereignty. We view this as a key differentiator for the company vis-a-vis its competitors. This is especially important as the WISeKey RoT serves as a common trust anchor, which is recognized by operating systems (OS) and IoT applications to ensure the authenticity, confidentiality and integrity of on-line transactions. With the cryptographic RoT embedded on a device, the IoT product manufacturers can use code-signing certificates and a cloud-based signature-as-a-service to secure interactions among and between objects and people.

We believe these features could be vital in opening up multiple business opportunities with various governments, international bodies, industrial companies which are wary of foreign government oversight and centralization of data on servers outside their jurisdiction. Also multinationals that need to comply with International Standards on the deployment of their IoT infrastructural are ideal candidates for WISeKey Trust Model. Amidst the threat of increasingly sophisticated data and online identity thefts, we think WISeKey's robust solutions should ensure data protection for their customers including individuals, enterprises & their IoT objects and government organizations.

We note that WISeKey is steadily diversifying across various geographies. The company has been expanding strongly in the US through channel partnerships with major global players such as CenturyLink (one of the top telcos in the US), SAP, Microsoft, The Bancorp and Samsung. Moreover, cloud hosting and IT services provider CenturyLink will resell WISeKey's cybersecurity solutions to the top 500 US companies, which should provide the latter with further penetration in North America. To make this deployment fully compliant with the US legislation on Cryptography and RoT, WISeKey and CenturyLink are currently creating a US rootkey located on a Secure Data center in Ohio, Columbus to serve the US market, in line with the "National Strategy for Trusted Identities in Cyberspace" (NSTIC), a US government initiative announced in April 2011 to improve the privacy, security and convenience of sensitive online transactions through collaborative efforts with the private sector, advocacy groups, government agencies and other organizations.

In addition, WISeKey sees further avenues for geographical expansion in Switzerland, Europe, Middle East, Asia and Latin America. Amongst new customer acquisitions, WISeKey's revenue concentration is low, given that the top 20 accounts in this category contribute just 20% of revenue, which is a key positive for a relatively small company such as WISeKey.

Inorganic growth to propel future growth

WISeKey has been seeking to build on its Vertical Platform solutions through strategic acquisitions and partnerships to drive top-line growth. Management expects potential acquisitions to add new verticals, products, services and geographies to its Vertical Platform solutions portfolio.

In one of its landmark acquisitions, in August 2016 (deal announced in May 2016), WISeKey signed a binding agreement to acquire VaultIC, INSIDE Secure's IoT integrated circuits and semiconductor business as the latter seeks to focus on its software security and technology licensing businesses. The transaction, worth CHF13.0mn (CHF2.0mn in cash and CHF11.0mn in bonds convertible into listed shares of WISeKey International Holding), has closed August 2, 2016. The INSIDE Secure businesses being acquired generated sales of USD35.0mn annually and is expected to contribute around USD8.4mn to FY2016E revenues. Through this deal, WISeKey aims to offer a comprehensive and trusted end-to-end cybersecurity platform targeting the high-growth IoT market. The acquisition will allow for cross-selling opportunities for WISeKey as INSIDE Secure's integrated circuits will allow WISeKey's RoT and digital certificates to authenticate devices. Management expects the deal to create a comprehensive vertical, trusted cybersecurity platform combining hardware, cryptography and software. In July 2016, WISeKey signed an agreement with the intention to merge with the Swiss company OpenLimit, a provider of software for electronic identities and signatures. WISeKey expects the deal to expand the company's cybersecurity and IoT platform and access to the German and EU IoT market.

WISeKey continues to hunt for further deals in Germany & other European countries and the US in the field of blockchain technology for peer-to-peer transactions, artificial intelligence, quantum technology and encryption. We believe WISeKey will continue to rely on acquisitions as part of the growth strategy for its Vertical Platform, thereby aiming to integrate its disparate technologies into an end-to-end chip-to-root solution.

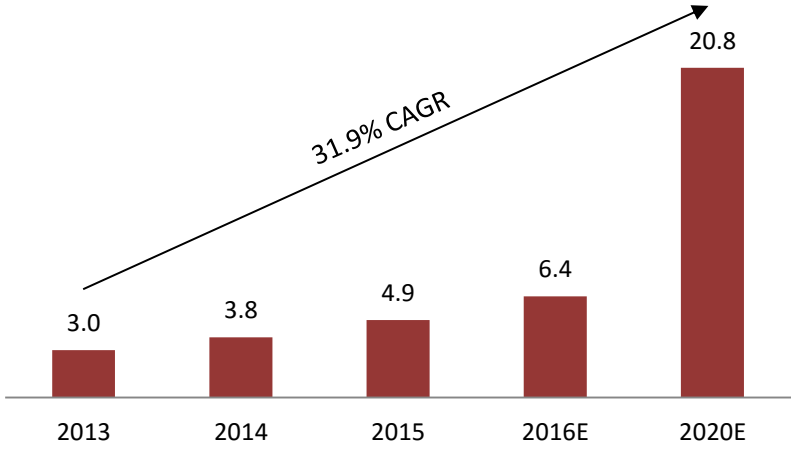
Exposure to high-growth markets offers substantial growth potential; IoT the key focus area

WISeKey's Vertical Platform solutions target a number of high-growth areas including mobile security & payments (via its partnership with Kaspersky for Mobile Security and MasterCard for payments), identity management and IoT, to name a few. The company is particularly focused on leveraging its Vertical Platform to serve the cybersecurity IoT market, an area in which it has taken major strides recently, thereby enabling the company to offer a comprehensive IoT ecosystem. We believe the deals with INSIDE Secure and OpenLimit have been made with a clear focus on the cybersecurity IoT market. We like management's move to acquire INSIDE Secure's assets and position itself as a vertically integrated Vertical Platform IoT solutions provider.

We think an important growth area yet to be fully monetized is WISeID Kaspersky, the Mobile Security offering between WISeKey and Kaspersky. WISeKey is also exposed to the mobile payments space. WISeKey's IoT technology has been used in Bulgari's intelligent mechanical watch to enable payments and other transactions without the use of a mobile phone or any internet-connected device. Segregating on the basis of a solutions portfolio, management expects the robust revenue growth in 2016 to be primarily driven by Cybersecurity, WISeAuthentic and IoT solutions.

According to a report from Bloomberg, the market for mobile transactions is projected to reach a staggering USD90bn in 2017, up from just USD12.8bn in 2012. According to Gartner, 20.8 billion IoT devices will be in use by 2020 compared to 4.9 billion in 2014, which equates to a compound-annual-growth-rate (CAGR) of 33.5% (2013-2020E CAGR: 31.9%). We believe WISeKey is well-positioned to take advantage of the multiple opportunities in its target markets.

Exhibit 1: Endpoints of the IoT by Installed Base



Source: Gartner, November 2015

Established operations and focus on strategic partnerships with major global players

WISeKey was established in 1999 and has thus been in operation for a reasonable time. The company uses a cryptographic RoT technology which is owned by OISTE, a Swiss foundation acting as the Trusted Party on the RoT generation. The RoT has already been installed across more than 2.6 billion devices. With a large installed base already, we believe WISeKey is poised to benefit from an increasing number of connected IoT devices (29.5 billion in 2020) as these devices require asymmetric identification which can only be provided by the RoT.

The company also has strategic partnerships with some major global companies including MasterCard, Hublot, Microsoft, Bulgari, The Bancorp Bank, Oracle, Samsung and SAP all of them using WISeKey Cybersecurity technologies.

With Bulgari, WISeKey is extending the monetization to over 1.5 million Bulgari clients paying EUR49.99 per year to subscribe to Bulgari Vault. WISeKey expects to monetise this ecosystem by allowing Bulgari to analyse the non-confidential data gathered during the process of use of the Bulgari Vault. On a separate note, although a longer term proposition, WISeKey could generate transactional revenues in the future on applications such as WISFans to monetize the fan-base of clubs such as FC Barcelona, which already use the application. We also note that the partnership with SAP to secure IoT Edge devices and the deal with CenturyLink to resell its cybersecurity solutions in North America could be key sources of revenue growth going forward.

Management expects the pro forma revenues from partnerships with SAP and CenturyLink to reach CHF35.0mn in 2017E from CHF5.0mn in 2016E.

COMPANY OVERVIEW

WISeKey offers digital security technology in the field of cybersecurity, digital identification and authentication of people & objects. The company has developed asymmetric encryption methods based on a unique RoT. The name of the foundation in which the RoT is held is OISTE/WISeKey. The RoT is a set of functions in the computing module that is trusted by the computer's operating system. WISeKey has patented this process in the US, which is currently used by many IoT providers.

The RoT serves as a common trust anchor, which is recognized by the operating system (OS) and applications, to ensure the authenticity, confidentiality and integrity of on-line transactions. With the cryptographic RoT embedded on the device, the IoT product manufacturers can use code-signing certificates and a cloud-based signature-as-a-service to secure interactions among objects and between objects and people.

RoT serves as a separate trusted computing hub controlling the trusted computing platform's cryptographic processor on a desktop, mobile device, wearable device or IoT in which it is embedded. The company's global RoT – located in Switzerland – ensures geopolitical neutrality and data sovereignty, which makes it easier for governments and corporations to rely on WISeKey for their IoT digital identity systems requirements. The company's technology ensures secure authenticated digital communication and data transfer between people and objects, both in relation to mobile and fixed-line internet transfers. The company's technology has been granted patents in the US, Singapore, Switzerland and Australia, and patents are pending examination in China, Canada, Japan, Brazil and India. Founded in 1999, WISeKey is the only cybersecurity company listed on SIX Swiss Exchange operating a Global RoT able to provide a comprehensive Vertical Platform chip-to-root. The company is headquartered in Geneva, Switzerland. The employee base has developed from 16 FTE in 2013 to 32 currently (including 21 full-time consultants) and is adding 70 more staff via the acquisition of VaultIC from INSIDE Secure, bringing the company staff strength to 102 in Q3 2016.

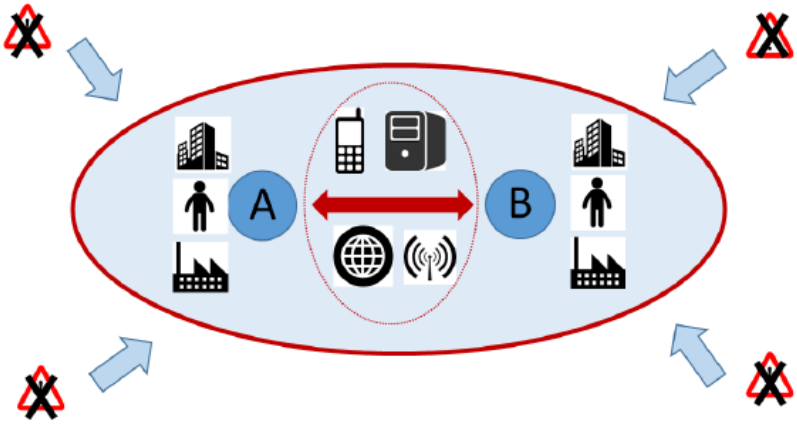
WISeKey's long-term history has led to the RoT being downloaded and embedded in more than 2.6 billion desktops, mobile browsers and IoT devices so far. In 2015, WISeKey announced co-operation agreements with Bulgari, Hublot, Kaspersky Labs and Samsung to implement its technology used to identify watches electronically and offer protection against counterfeiting. Over 1 million watches are digitally tagged using the company's technology. In addition, WISeKey and Bulgari launched the first intelligent mechanical watch using company's IoT technology, in 2015, which allows the watch to execute payments and other transactions without using a mobile phone or other devices connected to the internet. WISeKey launched with Bulgari the Diagono Magnesium Intelligent watch and the Bulgari Vault app allowing users to securely backup data online using WISeKey cybersecurity technologies and data storage on Swiss Alps.

With virtually limitless applications to a number of verticals, the Diagono Magnesium Intelligent watch using this unique secure wearable technology represents a huge value proposition to all Bulgari ecosystem members.

Product Offerings

WISeKey's entire offerings revolve around a Vertical Platform that ensures secure communication between "A" (a person, a device or an object or an entity) and "B" (a person, a device or an object or an entity) based on an encrypted authentication process that also offers protection against intrusion from outside.

Exhibit 2: Key Offering



Source: Company Data

The company's authentication and identification cybersecurity technology is based on a cryptographic rootkey that is owned by the International Organization for Secure Electronic Transactions (OISTE). OISTE has granted the company an exclusive perpetual license to use the cryptographic rootkey and develop technologies & processes based on OISTE's trust model.

The company provides its solutions through three business areas – Cybersecurity Services, IoT / Digital Brand Management (DBM) and Mobile Security.

Exhibit 3: Business Units

Cybersecurity Services	IoT /DBM	Mobile Security
• Protects digital communications & data with personal, corporate and server digital certificates • Protects corporate data with trusted archiving, invoicing	• Digital Item ID • Ensures authenticity of goods, online and physically, from the supply chain to the end user	• Digital Personal ID • Protects privacy by securing mobile phone communications, data and transactions
WISeSecurity	WISeAuthentic NFC Trusted	WISeWATCH WISeid WISeFans

Source: Company Data

Cybersecurity Products and Services

WISeKey offers the CertifyID and WISecurity product line to provide trusted IDs for persons and servers. WISeKey's technology can also be used as base for dematerialization solutions such as a secure archiving system that certifies the existence in time of sensitive data (such as smart contracts), and digital signature based transactional services.

WISeKey is one of the few players that can provide both PKI Technology and Trust Services, which can be used for enterprise and Government projects.

Internet of Things

As a special application of the well-proven PKI technologies, WISeKey has developed a special edition of its CertifyID technology, adapted to the requirements of the IoT, enabling customers to manage strong identities for connected devices.

WISeKey IoT platform goes beyond the issuance of identities and can be used to manage the security of data transactions, by protecting the messages sent by the connected devices. This will allow the central systems to verify that they are dealing with genuine devices and therefore control the new security risks for data theft and manipulation.

With the aim to provide trusted end-to-end cybersecurity solutions to its customers, WISeKey recently signed a binding agreement to acquire the secure IoT integrated circuit solutions and semiconductor business VaultIC from INSIDE

Secure for CHF13.0mn. INSIDE Secure's integrated circuits will allow WISeKey's cryptographic RoT and digital certificates to be hosted on a hardware vault that has received the certification to encrypt the communication and authenticate the devices. The transaction would include the transfer of products, technology, customer agreements and certain patents. More specifically, it would include the transfer of assets related to the development and sale of secure integrated circuits for the IoT market as well as a complete team in R&D, sales, marketing and support. This would enable WISeKey to offer authentication chips to their existing client base. INSIDE Secure's solutions have application for IoT, anti-counterfeiting, brand protection, EMV payment card and secure access. WISeKey also plans to leverage on the existing customer base of INSIDE Secure such as Cisco which uses INSIDE Secure's chips to authenticate their routers. WISeKey's management expects the acquisition to drive both short- and long-term revenue growth and also accelerate the strategy for global expansion. Due for completion in September 2016, the acquisition is expected to add c. USD8.4mn to WISeKey's FY2016 revenue.

Digital Brand Management

Under this category, WISeKey offers products for digital authentication for luxury products to reduce counterfeiting, as a specific approach for the IoT in device authentication and anti-counterfeiting. WISeKey provides WISeAuthentic along with NFC Trusted solutions to help users prove the authenticity of their products. Brand protection has become a strategic focus of WISeKey as advanced counterfeiting continues to challenge organizations. WISeAuthentic involves a non-duplicable digital certificate which is stored on a cryptographic smart chip embedded into a branded SmartCard. This allows manufacturers or resellers of luxury goods to prove the authenticity of the items to their customers, and for the customers to prove it to authorities and third parties.

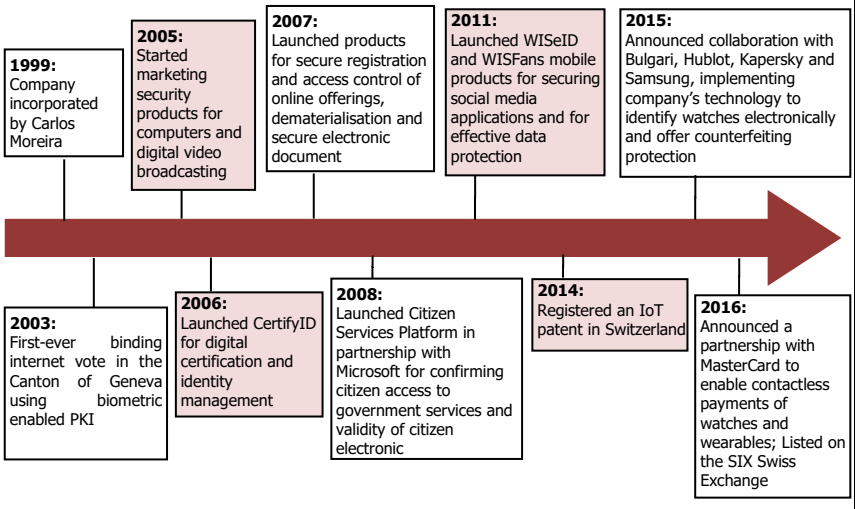
Mobile Security (MS)

The company started offering Mobile security line of products in 2012. It currently offers WISeID and WISFans under this business area. The products can be used by individuals and corporate organizations. Individuals can protect their privacy using digital personal IDs while using devices connected to cloud and using internet. Organizations can use these products to identify their customers and interact with them for the purpose of enhancing brand value and customize their marketing efforts.

Focus on the US market

WISeKey established an office in Silicon Valley in September 2015 to better serve its US target customers and establish strategic relationships with major partners. In April 2016, the company signed a definitive agreement with CenturyLink Inc, a communications, hosting, cloud and IT services company. Under the deal, CenturyLink will resell WISeKey's portfolio of cybersecurity solutions, including its MPKI technology and services to the growing enterprise and IoT markets in the US and globally.

Exhibit 4: Events Timeline



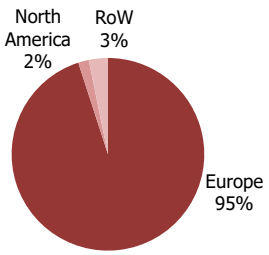
Source: Company Data

WISeKey was incorporated by Chairman and CEO Carlos Moreira in 1999. In cooperation with the Canton of Geneva and HP, WISeKey won the tender to provide the cybersecurity solutions for the first ever binding Internet vote, including through the use of a Public Key Infrastructure (PKI) and Quantum cryptography to secure the e-voting platform.

In 2005, WISeKey was nominated by Microsoft as one of the most innovative companies in Europe and signed an agreement with the US IT major to secure their identity ecosystem. In the same year WISeKey began marketing cybersecurity products and services via a licensing agreement for computers, mobile phones and digital video broadcasting with the establishment of a RoT for DvB Corporation. In 2006, WISeKey launched its CertifyID product acting as a Trusted PKI offering for digital certification and identity management. In 2007, WISeKey continued to grow its family of security products with solutions for secure registration and access control of online offerings, dematerialization and secure electronic document dematerialization. In 2008, the company launched its Citizen Services Platform in a partnership with Microsoft Corporation for confirming citizen access to government services and validity of citizen electronic IDs. WISeKey and Microsoft won against Google on a major tender in Spain in Bilbao to secure over 2 million citizens' IDs and their interactions with their local government. Between 2010 and 2012, WISeKey developed its Mobile Security suite and began marketing its WISeID app and desktop products and Social ID Fans (now marketed as WISFans) mobile products for securing social media applications and for effective data protection. WISFans started to be used in the sports communiity with deals for soccer teams such as Real Madrid, FC Barcelone, Flamengo, Swiss National Team, Alinghi, Oracle Team USA and the Bilbao basketball team. WISFans has beceome the reference on sport fans monetization stargeies allowing brands to engage their fans on social ecosystems, issuing asymetric keys to all fans to perform transctions on their mobile phones.

Over the last two years, WISeKey has been developing and commenced marketing and deploying its WISeAuthentic product for the security of luxury goods, artwork, pharmaceuticals, spare parts and VIP social networking. In 2014 WISeKey developed its Vertical Platform model integrating IDs and IoT into a solution now used for objects. In 2016 WISeKey signed a deal with SAP, the world's largest provider of enterprise applications. The collaboration aims to allow the integration of WISeKey's Managed cryptographic RoT secure IoT Edge Device with devices leveraging SAP HANA cloud platform for the IoT.

Exhibit 5: Revenue break up by geographic region (FY2015)



Source: Company Data

REVIEW OF FY2015 RESULTS

Fiscal Year ending 31 December (FY2015) was a transitional year for WISeKey as WISeKey International Holding (the listed company WIHN) was created end of 2015 to integrate all the Intellectual Property (IP) and assets of the group and consolidate the Vertical Platform model. The changes at the group level included the establishment of the Group's new holding company (WISeKey International Holding AG) in December 2015 and the strategic repositioning of the Group towards a listing on the Swiss Market in Q1 2016. This was seen as an important event to increase WISeKey's visibility towards global collaboration partners.

WISeKey's revenues for FY2015 were USD2.3mn as compared to USD3.5mn for FY2014. The fall in revenue is attributable mainly to the European region (-33.6% y-o-y, c.95% of revenue) and North America (down by 67.4%). Against this, revenue marginally went up in the RoW segment (up by 4.8%). The majority of the revenue contribution was from cybersecurity IoT sales, which is a new revenue model introduced by the Group in 2014/15. The operating loss substantially decreased from USD32.4mn in 2014 to USD7.5mn in 2015. The company raised another USD7.7mn in equity to tap growth opportunities and in anticipation of its listing on the SIX Swiss Exchange. In addition, as announced in January 2016, WISeKey secured a CHF60.0mn equity financing facility from institutional investor Global Emerging Markets (GEM). This facility provided the company with an option to issue and sell shares to GEM over the next 5 years of up to CHF60.0mn. Over the last 10 years, WISeKey has raised a total of CHF120.0mn and this facility brings the total capital raised to CHF180.0mn under current commitments. Therefore, WISeKey plans to take advantage of substantial organic and acquisition-driven growth opportunities to further develop its Vertical Platform and extend the reach of its identity ecosystem to new markets and countries.

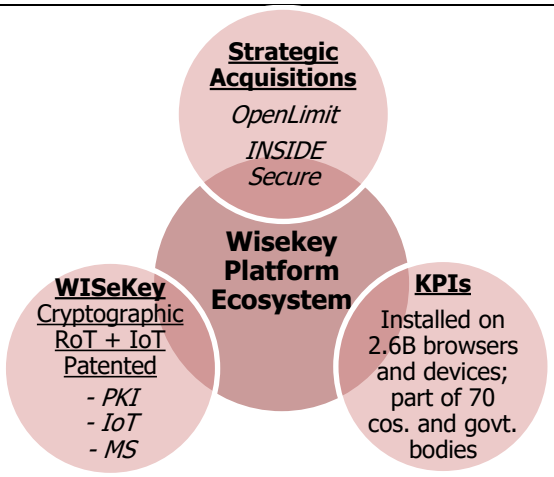
WISeKey signed material contracts & cooperation agreements with global customers and strategic partners in 2015 as well as in the first six months of 2016. As such, WISeKey has secured a significant portion of near-term projected revenues with clients such as MasterCard, Hublot, Microsoft, CenturyLink, Bulgari, SAP and Samsung, and we expect WISeKey's FY2016 revenue to reach USD25.8mn.

BUSINESS MODEL

WISeKey aims to be a global Vertical Platform providing advanced cybersecurity technology and services that authenticate and protect digital identity across personal, business, objects and administrative transactions online. The company offers its solutions through a technological software platform that secures communication between two parties (a person, a device or an object or an entity) based on an encrypted authentication process. This also offers protection against intrusion from outside. The authentication and identification of the cybersecurity technology and platform is based on a cryptographic rootkey that is owned by OISTE. OISTE has granted the company a perpetual license to use the cryptographic rootkey and develop technologies & processes based on OISTE's Trust Model. WISeKey has embedded its cryptographic rootkey RoT, providing military-grade security to users, already in over 2.6 billion browsers, sensors, wearables and IoT devices, providing the basis for substantial growth. The company is now focusing on consolidating its current position through vertical acquisitions (such as INSIDE Secure) and therefore, to grow inorganically.

With this new model WISeKey has become one of the fastest growing cybersecurity companies in the world. The company is a leading Swiss information security and identity management software and services company. WISeKey is currently deploying large scale IoT digital identities ecosystems and has become a pioneer of the 4th Industrial Revolution movement launched this year at the World Economic Forum at Davos. WISeKey's Swiss-based Cryptographic RoT integrates wearable technology with secure authentication and identification, in both physical and virtual environments, and empowers IoT and wearable devices to become secure transactional devices. WISeKey has patented this process in the US as it is currently used by many IoT providers. WISeKey is a Global Growth Company Partner of the World Economic Forum.

Exhibit 6: Business Model



Source: Company Data

Cybersecurity services

Sales of online trust solutions are made on the basis of the number of cloud accounts, e-IDs or transactions; branded service fee; an agreed upon monthly or annual fee. Organizations which install online trust solutions products are billed as per the software purchased and the volume of contracted services. Enterprise mobile security products are billed based on the numbers of devices that get installed with the solution. There is an upfront set-up cost and a recurring revenue stream for service as needed. For the web-security, the product is purchased with managed service fees and setup & software fees.

The company sells Cybersecurity Services products to resellers and directly to organizations and consumers. The resellers are companies already established in the IT security sector, which, in turn, sell the products to consumers and can be engaged to help with installation. Direct sales to consumers are mainly conducted through the online merchant website, which allows immediate credit card payments.

WISeKey has signed a strategic cooperation with SAP allowing increased security of IoT devices when connecting to SAP solutions for IoT. Having sensors connected to everything does not necessarily enable monetization or customer value. Companies and consumers can realize value and enable monetization when they can certify that they are receiving authenticated and secure sensor data, gain insight from it and propose appropriate actions as needed.

This new collaboration with SAP is indicative of WISeKey's broad and continuously expanding cybersecurity IoT offerings, as the company is placing significant emphasis on strategic relationships to increase penetration and boost sales with established enterprise players such as SAP. Securing data communications from edge devices to the SAP HANA cloud platform for the IoT and SAP solutions for the IoT is a prerequisite for any bi-directional enterprise IoT use case. By working with WISeKey, SAP is continuing to offer itscustomers options for ensuring the validity and scalability of sensor data powering SAP IoT platform and solutions.

CertifyID Digital Certificates (DC)

CertifyID DC can be purchased directly through the WISeKey website or indirectly through resellers who license it. Customers who are then linked to resellers can also order their certificates through the portal. Once an order is accepted, WISeKey processes the request and issues the certificate following the successful validation procedure according to the SSL certificate policy.

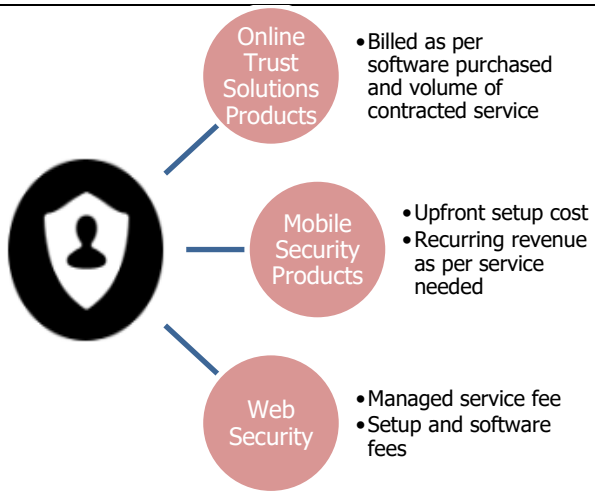
WISeKey also provides Digital Certificates as a freemium service via its WISeID app. WISeID acts as a dual factor authentication technology that sits on top of the WISeKey Vertical Platform.

The WISeID Kaspersky Lab Security cyber-resilience edition that uses digital identification to lock personal data such as account usernames and passwords, credit card numbers and access PINs into a secure personal data organizer, creating accountable identities for online activity while the data itself remains protected in a secure cloud vault.

Without mobile security software, users are vulnerable to all these threats and more. The WISeID Kaspersky Mobile Security SDK includes a robust and proven solution for protecting mobile phones against security threats. The SDK's inclusion in the app delivers advanced security features such as web & network protection, device protection and risk detection to smartphones, offering users an effective layer of self-defense.

Among other things, WISeID keeps passwords in an encrypted vault, generates hard-to-crack passwords, and synchronizes data between computers and devices on multiple platforms, using secure cloud storage. The vault can be unlocked only with the user's Master Password and/or defined pattern, with additional protection provided through facial recognition authentication. WISeID can be accessed online though a single click.

Exhibit 7: Revenue model for Cybersecurity services



Source: Company Data

Internet of Things

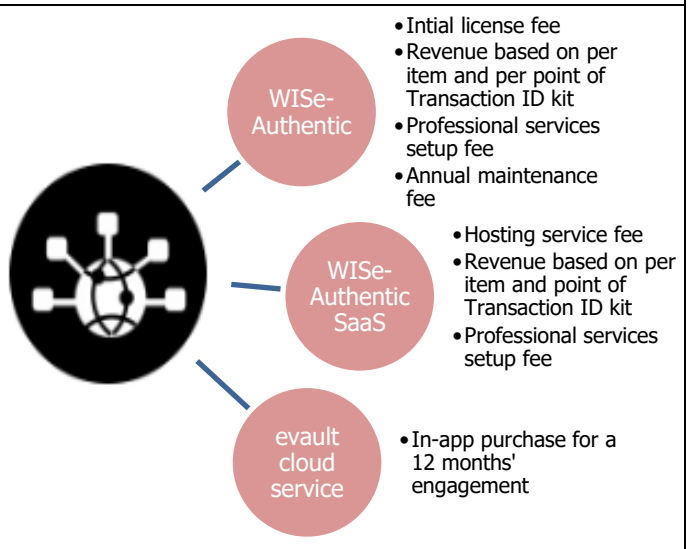
WISeKey follows an adapted business model of CertifyID for the new IoT projects, considering the potentially huge volumes in terms of individual devices to be provisioned with an Identity. Customers can choose among managed and on-premises deployment, depending on their business needs. Special requirements and adaptations for IoT messaging processing are evaluated "ad-hoc".

Digital Brand Management

WISeAuthentic licenses consist of an initial license fee, a per item (recurring as based on the yearly production) and per point of transaction ID kit including a crypto device and digital & optional USB reader, a professional services set-up fee, an annual maintenance fee for the respective licenses. This model may change in case of Software as a Service (SaaS), as the license rental and respective maintenance would be embedded into the hosting services fee, rest remains unchanged. Engagements with clients are multi-year contracts (mostly 2 to 3 years). eVault cloud services are based on an in-app purchase for a 12 months' engagement contracted by the consumer for 3GB extendable storage.ISeKey follows an adapted business model of CertifyID for the new IoT projects, considering the potentially huge volumes in terms of individual devices to be provisioned with an Identity. Customers can choose among managed and on-premises deployment, depending on their business needs. Special requirements and adaptations for IoT messaging processing are evaluated "ad-hoc".

WISeKey contracts directly with luxury manufacturers for the sale of Digital Brand Management (DBM) products. The customers are charged based on the number of products they wish to authenticate. The company currently markets DBM products to luxury brands, such as luxury watch manufacturers. In addition, the company plans to start marketing these products to manufacturers in the pharmaceutical and aeronautics sectors.

Exhibit 8: Revenue model for IoT & DBM



Source: Company Data

For sale of the WISeID product, the company has entered into strategic partnerships with various companies so that they can install solutions on their products. Specifically, WISeKey has strategic partnerships and collaborative relationships with Microsoft Corporation. WISeID generates revenue based on the number of subscribers to its premium offerings. Customers can use WISeID for free and can take advantage of premium features through purchases within the applications or through annual subscriptions. WISFans generates advertising revenue on the basis of the number of applications downloaded, the value of the brand partner, the number of ad impressions, push notifications and other mobile analytics. The company also enters into agreements with companies to provide the application for free to consumers and revenue is generated through active use of the application by fans or customers.

WISeKey has secured a significant portion of near-term projected revenues with accounts such as MasterCard, CenturyLink, Bulgari, SAP and Samsung, and we expect WISeKey's FY2016 revenue to reach USD25.8mn. The bulk of the projected revenue thus evolves from WISeAuthentic and IoT solutions, benefitting from the strategic partnerships to develop and market products and solutions with large organizations. The most significant growth areas will thus be to provide cybersecurity and secure chip technology to IoT solutions (e.g. for industrial utilities), identity management solutions on mobile devices and mobile security for electronic payment services. Moreover, if the opportunities arise, the company intends to grow through acquisitions in order to reduce the time it takes to bring updated and new products to market and expand the reach of the WISeKey cybersecurity platform. All this will require deploying further high outlays, thereby expanding the company's capacities and international footprint.

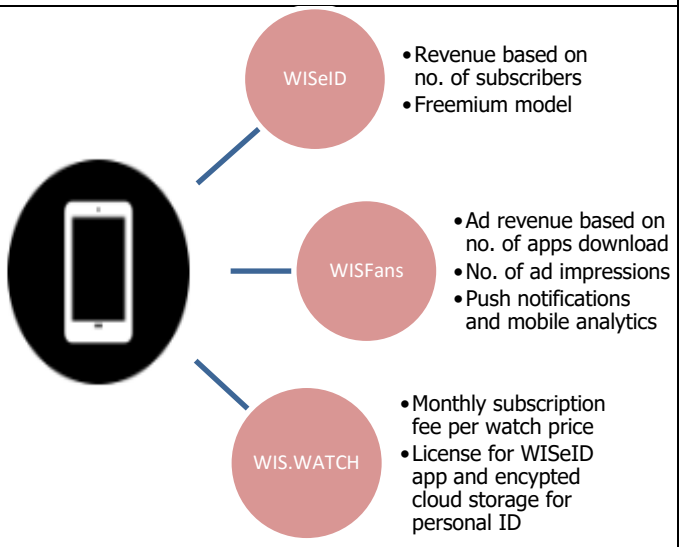
In case of WIS.Watch, a Near Field Communication (NFC) watch sends a secure digital identity via NFC technology to the WISeKey Mobile Phone App which unlocks the personal data wallet and activates the phone. WISeKey charges a monthly subscription fee per watch price, besides the license for WISeIDApp and encrypted cloud storage for personal ID.

The company, along with Bulgari, launched the Diagono Magnesium Intelligent watch and Bulgari Vault app concept in 2015, which together allow users to securely backup their data online using WISeKey cybersecurity technologies and allow for data storage on Swiss Alps. An amount of Euro 49.99 per year per client is being charged. Bulgari has 1.5 million registered clients (buying Watch and using Bulgari Vault app). The revenue is shared by Bulgari (1/3) and WISeKey (2/3). Bulgari plans to gradually expand the services on the Bulgari Vault app and increase its Average Revenue Per User (ARPU).

With respect to Bulgari Magnesium, WISeKey expects to earn USD26/unit for 250,000 watches. Expected revenue per watch including WISeIDvault and cloud services is in the range of USD10-USD50/watch. The company also plans to extend the services to 25 million LVMH luxury objects and 150 million perfumes and cosmetic items.

During 2015, WISeKey also signed a new deal with Bulgari allowing the former to provide technology to the major brands of LVMH group.

Exhibit 9: Revenue model for Mobile Security



Source: Company Data

BUSINESS UNIT OVERVIEW

WISeKey has divided its solutions in three business areas including Cybersecurity Services, IoT / DBM and Mobile Security.

Cybersecurity services

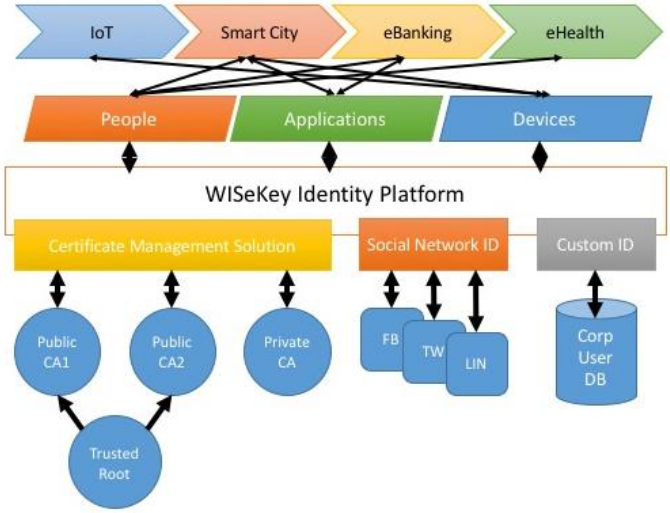
The company started offering its online trust solutions of Cybersecurity services in 1999 to provide trusted IDs for persons and servers. WISeKey currently offers CertifyID and WISecurity within this business area.

CertifyID – Digital Identity

WISeKey CertifyID can be used to create digital signatures and as proof of identity in significant value transactions and interactions such as e-voting, healthcare, payment and clouds. It helps organizations by securing data, permitting secure messaging and reducing paper needs. The product uses the company's trusted root technology to secure a person's digital identity.

CertifyID TrustCenter Service allows organizations to deploy a corporate PKI or CA under the WISeKey Root CA, integrated in its trust model and it therefore inherits the recognition and accreditation.

Exhibit 10: CertifyID Global Identity platform



Source: Company Data

WISecurity – Digital Certificates

WISecurity protects online communications and data with personal, corporate and server digital certificates. It provides dematerialisation solutions, including a secure archiving system that certifies the existence in time of sensitive data (such as contracts) and e-signature based invoicing services.

The company has 10 years of experience in projects related to digital certificates and identities. It operates a secure PKI to provide certification services to end-users and organizations. It offers the following products:

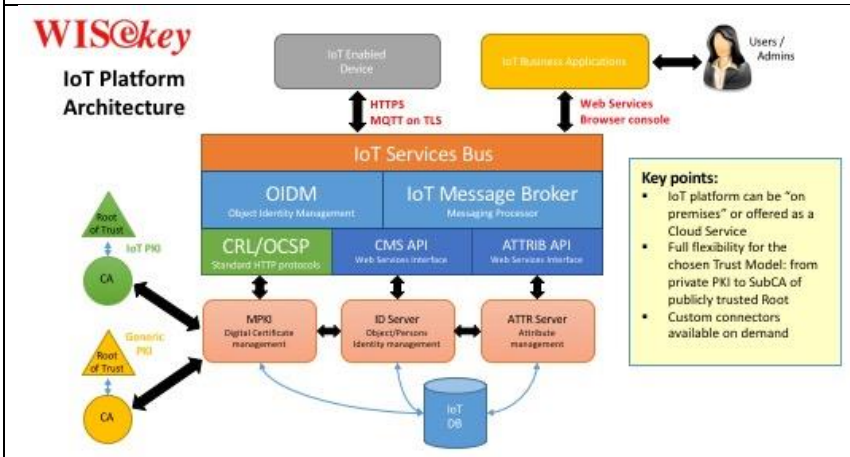
- SSL certificates: Protect servers and applications, ensuring the confidentiality of transactions over the web
- Personal certificates: For secure authentication, digital signatures and e- mail protection, compatible with desktop and smartphones
- Qualified certificates: For PDF document signing. Qualified certificates are included in the Adobe Accredited Trust List, allowing customers to digitally sign documents, fulfilling all the security requirements from Adobe
- Managed PKI: Solutions for corporations required to issue digital certificates to their employees and customers; optimizing electronic transactions by using digital signatures. The MPKI platform is used by clients that do not wish to host their Certification Authority within their own data centre. It is a service-based solution that is hosted and maintained in the company's data center infrastructure in Switzerland.

Internet of Things

WISeKey provides a full set of solutions aiming to cover the new needs of IoT projects, where it is equally important to make a provision of the identity than putting it in value by integrating new security mechanisms into the IoT data transactions.

With WISeKey's technology, customers can build fully-fledged IoT solutions to protect not only the identity of the objects but also the data transferred during its life-cycle.

Exhibit 11: IoT Platform



Source: Company Data

Digital Brand Management

The range of IoT and DBM products provided include digital authentication for luxury products including luxury watches, high-end glasses, smart phones and designer clothes. Manufacturers can use WISeAuthentic to reduce counterfeiting and certify the authenticity of their products.

Using a combination of established RoT and NFC technologies, consumers can securely use intelligent devices as the key to the rest of their digital universe.

Exhibit 12: IoT Opportunity for Wearables

Source: Company Data

WISeAuthentic (WA)

WA Anti-Counterfeiting

WISeAuthentic offers a digital certificate of authenticity for luxury or other valuable items, to protect them against counterfeiting. It is based on the principle of the traditional paper-based certificate, but instead of using a forgeable piece of paper, a non-duplicable digital certificate is stored on a cryptographic smart chip embedded into a branded SmartCard. This allows manufacturers or resellers of luxury goods to prove the authenticity of the items to their customers, and of course, for the customers to prove it to authorities and third parties, even over the Internet.

WA Transactions

With WISeAuthentic, when an item is sold, its warranty is activated online using the shop's official reseller SmartCard and reader. Information stating which shop sold which item and when is sent automatically online to the manufacturer. The manufacturer can therefore ensure they receive accurate sales information that can then be used for analyzing the impact of marketing activities and estimating the stock of resellers. This also provides a valuable tool for gaining control over the gray market.

WISeAuthentic also allows the implementation or integration of a unique, certified online retail shop and / or a certified auctioning platform.WA for CRM Enrichment

WISeAuthentic can also allow the manufacturer to have direct contact with the end consumer by offering the item owner the possibility to register online. The owner then benefits from being given access to certain functions, for example being able to update the status of the item, without affecting the worth of the original certificate. Owners of a WISeAuthentic certified item can access an owner's VIP club online, allowing the vendor to provide them with innovative value-added services using direct marketing facilities. Access is reserved for owners of certified objects, as the SmartCard is used to log in to this optional service.

The company has recently signed a Memorandum of Understanding (MoU) with Samsung to provide its RoT technology to Samsung IoT and NFC chips, allowing Samsung IoT to add asymmetric keys and digital certificates on their chips at the hardware level to encrypt the communication and authenticate devices.

NFC Technology

During 2015, the company initiated various product developments including employment of NFC tags which can be embedded into products across markets, from consumer goods to manufacturing. Along with supporting WISeAuthentic encryption technology, these tags allow authentication of genuine products for the life of the item, control the grey market, provide easier sales monitoring and create a direct marketing channel between brands and consumers.

Exhibit 13: NFC Trusted technology Variety of Form Factors

Source: Company Data

In 2015, the company also signed a strategic project with the Bulgari Group, enabling Bulgari to offer a mechanical watch that can be connected to the internet and can be used as an authentication device to open the Bulgari vault mobile application.

Mobile Security

The company's Mobile Security products provide users with digital personal IDs to protect their privacy while using mobile phones, tablets, laptops and other devices that make use of cloud and are connected to the internet. These products can be used by organizations to identify their customers and interact with them to add value to their brand and customise their marketing efforts. Under this vertical, the company offers products, including WIS.WATCH, WISeID and WISFans.

WIS.WATCH

WIS.WATCH connects with the users' smartphone and offers WISeID to protect their Personally Identifiable Information (PII). The cryptographic key that is stored on the watch can then be used for many other applications including unlocking doors and electronic locks at home and at work.

Exhibit 14: WIS.WATCH technology

Source: Company Data

WISeID – Secured Personal Data

WISeID protects personal data by giving users encrypted, portable storage for sensitive data which can be accessed by the user with secure credentials. It requires a multifactor authentication process which includes strong password generation, dot pattern recognition and biometric face authentication. Large organizations can use WISeID to bring mobile applications to their consumer base.

WISeID offers the following features:

- Secure and powerful password management
- Protected sign on to websites
- Safe security: 256 bit AES, PBKDF2 encryption keys
- Personal cloud solution: Keeps an encrypted backup of the user's data in a protected datacenter in Switzerland
- Syncs data among devices
- Works on multiple devices including iPhone, iPad, Android, Mac and Windows PCs and Kindle

Exhibit 15: WISeID

Source: Company Data

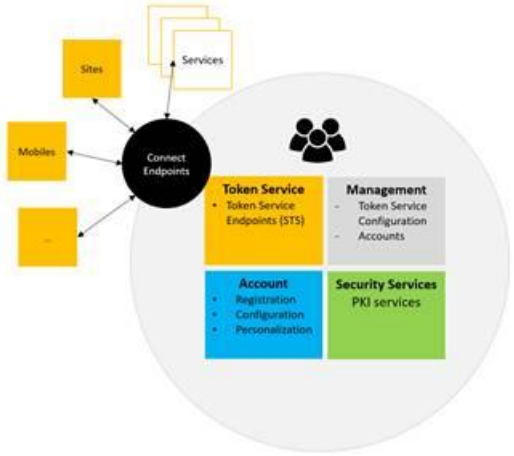
WISFans – CRM Enrichment

WISFans keeps fans engaged on and off the field through a digital 'clubhouse' ecosystem that collects and stores content including blogs, match reports, videos, photos, fan-supported social campaigns, Twitter, Facebook and sports forums, and adds ongoing content provided by the team and its players.

WISeID Connect – Federated Identity solution

To address new mobile and decentralized applications and services requirements, while maintaining the highest security level, WISeKey has developed a federated platform that combines both the PKI technologies with open standard communication protocols, including WS-Federation, OpenId, OAuth. This platform allows any application and service to delegate the authentication and authorization and leverage secure services such as encrypted communication, digital signature of operations and data. The platform manages the identity and security token lifetime and enforces trust and privacy with private key technology. The identities and private keys are combined to strongly identify people and objects, ensure authenticity and establish trusted communication in a secure environment.

Exhibit 16: Identity Federation



Source: Company Data

WISePhone – Secure voice communication solution

The WISePhone solution provides high-level encryption in voice calls performed from smartphones, dramatically reducing the risks of letting unauthorized parties to eavesdrop on the conversation contents.

The innovative approach that WISeKey brings into this domain is aimed at simplicity and ease of adoption of this technology. WISePhone users don't need to buy specific devices, rather just to install the WISePhone App on their smartphone and start performing secure calls with other WISePhone users

WISeKey is revamping the full WISePhone product line for a new major version in 2017, which will be integrated with the WISeID App and identity system, and also allow encrypted text instant messaging.

WISEKEY PRODUCTS IN END USER INDUSTRIES

Cybersecurity services

WISeKey sells its cybersecurity products to resellers and directly to organizations and consumers. WISeKey's resellers are companies already established in the IT security sector, such as systems integrators and internet service providers, including companies like ZyTrust S.A. and CenturyLink. These resellers sell the WISeKey products to consumers. Direct sales to consumers are mainly conducted through the company's online merchant website, which allows immediate credit card payments. The platform is tailored to address the key cybersecurity requirements of organizations, retail and government customers.

In May 2016, the company entered into an agreement with CenturyLink that enables the latter to resell WISeKey's cybersecurity solutions (including its MPKI technology and services) to businesses worldwide.

Internet of Things and Digital Brand Management

DBM products are sold to luxury product manufacturers and retailers. Manufacturers install the WISeKey cryptographic RoT technology and sell the pre-installed product to retailers and consumers. The technology is embedded in over 2.6 billion desktops and mobile browsers as well as in IoT devices. The company's customers in this product range include Bulgari, Tag Heuer, Hublot and Dior S.A. The company has digitally tagged over one million watches with its technology.

In the last week of July 2016, WISeKey signed an MoU with OpenLimit, a Swiss-based software company, which develops solutions for secure data communication, to combine the business of OpenLimit into WISeKey. Thus WISeKey will become the surviving entity. The combined portfolios of WISeKey and OpenLimit will enable WISeKey to provide more comprehensive solutions to the IoT market. The merger will also give WISeKey access to OpenLimit customers, in particular in Germany and other large and more mature markets in Europe. The agreement will also reinforce WISeKey's workforce with OpenLimit's 65 employees located in Germany.

In July 2016, the company announced that Bulgari has licensed the company to develop and offer BVLGARI VAULT App used for the secure storage of personal data such as account usernames and passwords, credit card numbers and access PINs. The application is a customized version of WISeID.

Also, in July 2016, the company entered into partnership with Microsoft CityNext, a global initiative that harnesses ideas, energy and expertise of a city's people. It combines a network of global partners and Microsoft's successful education, healthcare, and social programs and helps cities plan for and embrace the future. Under the partnership, WISeKey's RoT will be used to implement city cybersecurity projects to protect government infrastructure including traffic lights, smart parking solutions, power grids and smart utility meters, from potential cyber attacks.

The company has recently signed an MoU with Samsung to make available its cryptographic RoT to Samsung IoT and NFC Chips. This allows Samsung to add asymmetric keys and digital certificates on their chips at the hardware level to encrypt communication and authenticate devices. Asymmetric encryption, also known as public key encryption, utilizes a pair of keys – a public key and a private key. If a user encrypts the data with the public key, only the holder of the corresponding private key can decrypt the data, hence ensuring confidentiality. It differs from the symmetric encryption, which involves encryption and decryption operations utilize the same key. For two communicating parties using symmetric encryption for secure communication, the key represents a shared secret between the two.

Payments Capabilities

In February 2016, WISeKey announced a partnership with MasterCard to enable contactless payments of luxury brand watches and wearables. The partnership adds new devices and brands to the ongoing MasterCard programs that bring payments to any consumer gadget, accessory or wearable, from fitness bands to refrigerators. MasterCard will integrate its payments technology with WISeKey's cryptographic RoT for IoT and NFCTrusted technology solutions, providing consumers with the freedom to securely shop using their watch or other wearable devices. The partnership presents both companies with additional eCommerce and marketing opportunities for luxury wearable devices and watch manufacturers. This new product enabling payment capabilities with WISeKey platform connected

to the MasterCard Tokenization platform (provisioning a token into the wearable enabled from the credit card credentials) will be released at the beginning of 2017 with Bulgari as the first customer.

In 2015, WISeKey and Bulgari launched an intelligent mechanical watch using WISeKey's IoT technology, which allows the watch to execute payments and other transactions without using a mobile phone or other devices connected to the internet. The cryptographic key installed in the Diagono Magnesium intelligent watch can be used for various purposes, including unlocking Bulgari Vault app or paying for goods with NFC enabled contactless payment systems. WISeKey expects to earn revenues amounting to USD10-50/watch (including revenue from services such as WISeIDvault and cloud services). The technologies are to be installed in all wearables with a market amounting to an estimated USD1.7tn.

Exhibit 17: Bulgari Diagono Magnesium Wrist Vault

Source: Company Data

Mobile Security

The company has strategic partnerships with various companies so that they can install WISeKey solutions on their products including WISeID and WISFans. The company has sold its products to a number of professional sports teams and leagues including Real Madrid, Barcelona, SFV ASF Swiss Nati, Bilbao Basket, Vasco da Gama and Oracle Team USA. WISeKey generates revenue based on the number of subscribers to its premium offerings.

In March 2016, WISeKey and Kaspersky Lab launched 'WISeID Kaspersky Lab Security', a cyber-resilience app. The app integrates technologies from both companies to offer mobile users a safe and reliable mode for mobile communications and transactions. It locks personal data such as account usernames and passwords, credit card numbers and access PINs into a secure personal data organizer, creating accountable identities for online activity, while the data itself remains protected in a secure cloud vault. The app can be used on various platforms including iPhone, iPad, Android, Mac OSX, Windows and Kindle.

BUSINESS STRATEGY

One of the early entrants in the cybersecurity space, WISeKey has embedded its cryptographic rootkey RoT, providing military-grade security to users, already in over 2.6 billion browsers, sensors, wearables and IoT devices, providing the basis for substantial growth.

Entered into new contracts ensuring steady flow of revenue

The company has signed material contracts and co-operation agreements with global customers and strategic partners, securing a significant portion of projected revenues with accounts such as MasterCard, Microsoft, The Bancorp, CenturyLink, Hublot, Bulgari, and Samsung, corresponding to an expected annualized turnover of CHF70.0mn in 2016.

Bolstered financial position to enable inorganic growth

In early 2016, the company secured a CHF60.0mn equity financing facility from a consortium of international institutional investors led by GEM, which was followed by the listing on the SIX Swiss Exchange on March 31, 2016. The company intends to use the funds to grow through acquisitions in order to reduce the time it takes to bring updated and new products to market and expand the reach of the WISeKey cybersecurity platform. WISeKey aims to provide end-to-end 'chip-to-root' solutions to its customers by acquiring established businesses in complimentary verticals and hence, capitalize on the rapidly transforming IoT market.

New Product Families

WISeKey is currently deploying large scale IoT digital identities for wearables using its trusted NFC technology. This technology integrates wearable technology with secure authentication and identification, in both physical and virtual environments, and empowers wearable devices such as smart watches, bands, ear-pods, jewelry, eyeglasses, etc. to become transactional devices. Embedding digital certificates into wearables with WISeID NFCTrusted tags, using the WISeKey PKI and the OISTE global rootkey, enable consumers to interact securely with nearly any IoT object or transactions in a trusted way.

NFCTrusted authentication tags can incorporate a WISeKey cryptographically secure digital certificate to prove authenticity. NFCTrusted tags can be embedded in virtually any product, piece of equipment or common household item, and users can verify authenticity with an NFC-enabled smartphone, watch, connected device or other mobile device. This technology not only optimizes security and convenience, but also eliminates the need for special readers or other equipment for tag authentication by using proof of presence. Convenience offered by the product allows the company's to use NFCTrusted tags in diverse markets to support a variety of IoT applications.

Focus on growing in the US and globally

In September 2015, WISeKey opened an office in Silicon Valley and signed a reseller agreement with CenturyLink, a global communications, hosting, cloud and IT services company, wherein CenturyLink agreed to integrate WISeKey MPKI solutions with its offering and selling it to major global companies and US government agencies. The combined offering will provide CenturyLink's customers with a comprehensive cybersecurity solution for their managed security needs.

With the new partnership with CenturyLink, WISeKey is able to provide its technology to Top 500 companies in the US via an MPKI platform designed to meet the requirements of clients that do not wish to host their certification authority within their own data center. CenturyLink provides the infrastructure, while WISeKey provides the technology.

The company also entered into collaboration with SAP, which allows the integration of WISeKey's Managed Cryptographic RoT secure IoT Edge device with devices leveraging SAP HANA Cloud Platform for IoT. WiseKey and SAP collaborated on the definition of a solution offering that best meets SAP's IoT customers' needs.

Further collaborations with other security service companies are expected, including in Asia (particularly India and China), to expand WISeKey's international footprint.

Strategic acquisitions

WISeKey recently signed a binding agreement to acquire the secure IoT integrated circuit solutions and semiconductor business from INSIDE Secure for CHF13.0mn. INSIDE Secure's integrated circuits will allow WISeKey's cryptographic RoT and digital certificates to be hosted on a hardware vault that has received the certification to encrypt the communication and authenticate the devices. INSIDE Secure's product portfolio provides a compact, cost-effective design that will enable WISeKey to create IoT chips and NFC tags small enough to be available in a variety of forms to accommodate the shape of various IoT products.

According to a report published by Markets and Markets, the IoT security market is expected to grow from USD6.9bn in 2015 to nearly USD29.0bn by 2020, thus growing at an annual rate of 35% over the next five years. Related to the substantial IoT market growth, the cybersecurity IoT market is booming as devices that are accessible from TCP/IP networks face regular attack. WISeKey's cryptographic RoT and INSIDE Secure's technology enable the wearable devices to connect safely and make secure payments and other transactions. This enables IoT devices to be identifiable with digital identities and evaluate themselves and each other via a trusted platform and blockchains before agreeing to establish a telecommunications session.

The activities of INSIDE Secure to be acquired for IoT, anti-counterfeiting, brand protection, EMV payment card and secure access generated pro-forma revenue of USD33.6mn in 2015. The acquired business is expected to contribute c. USD8.4mn to WISeKey's FY2016 revenues.

The acquisition would include the transfer of products, technology, customer agreements and certain patents. More specifically, it would include the transfer of assets related to the development and sale of secure integrated circuits for the IoT market as well as a complete team in R&D, sales, marketing and support to WISeKey.

Strategic Relationship with OISTE

The cryptographic rootkey RoT used by WISeKey is owned by OISTE, a member of the United Nations' Economic and Social Council (ECOSOC), acting as a trusted third party and non-for-profit entity in charge of ensuring that the RoT remains neutral and trusted, and located in Switzerland as an independent, neutral jurisdiction. The name of the RoT is OISTE/WISeKey, as shown in all major current browsers that embed the rootkey.

OISTE has received special consultative status from ECOSOC promoting a "Switzerland on the internet" to provide net cloud neutrality. OISTE has granted WISeKey a perpetual license to exclusively use the cryptographic rootkey and develop technologies and processes based on OISTE's "Trust Model". The perpetual license agreement can only be terminated under limited circumstances, including if WISeKey were to move from the Trust Model developed by OISTE and/or changing the location of the RoT from Switzerland to another country.

WISeFans – An Important Focus Area

The company has been working with major sports franchises to gain from opportunities that the world of sports presents. WISeFans offers dynamic digital marketing strategies for sports clubs based on a "freemium" revenue model. Under such a model, WISeKey enters into agreements with companies to provide the application for free to consumers. Revenue is then generated through active use of WISeKey's applications by fans or customers. However, revenues generated through this "freemium" model have been insignificant to date and, while not expected to be a key revenue generator in future, this activity helps to increase WISeKey brand awareness and visibility across broad (fan) audiences. It also enables the clients to interact with their fans and leverage the huge fans' database by effectively channelising their marketing efforts.

Agreement with Bilbao Basket built the first global community and social media content in basketball.

The WISFans Bilbao Basket app

App lets fans follow Solar Impulse's flight; fans engage in real-time with the first solar plane to ever fly around the world.

The WISFans Solar Impulse HD app

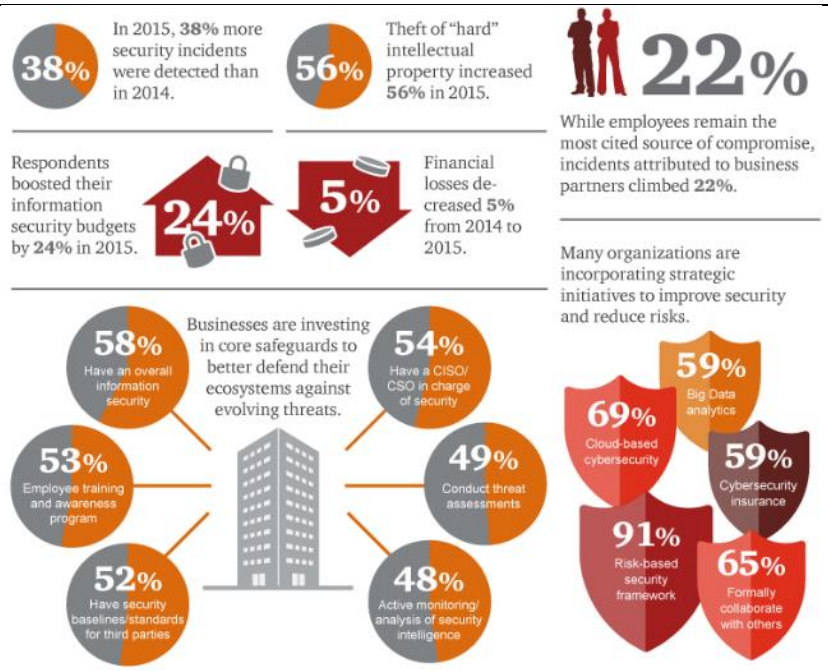
Agreement with Team Oracle USA – the app allows fans to follow the team and engage in real time.

The WISFansOracle Team USA app

INDUSTRY OVERVIEW AND COMPETITIVE LANDSCAPE

WISeKey currently operates in the cybersecurity market with focus on three main businesses: Cybersecurity service, IoT/DBM and Mobile Security. In general, the Cybersecurity market is fragmented, but largely dominated by several global security companies including VeriSign, Symantec, FireEye, Red Hat Software, VASCO Data Security, Zix Corp. and Easy Solutions. These large enterprises already have technical and financial resources and broad customer bases that allow them to bring competitive solutions to the market.

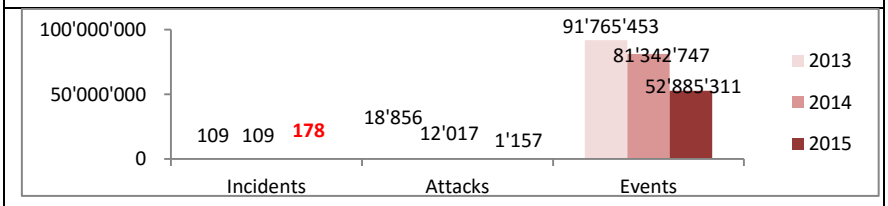
Exhibit 18: Cybersecurity at a Glance



Source: PwC

Cybersecurity, digital identification and authentication of people and objects is a rapidly growing sector owning to relentless attacks from cyber criminals, spies, terrorists or political hacking groups that businesses and governments are confronting. According to IBM Security Services, companies it monitored experienced 81-91 million cybersecurity events per year in 2013 and 2014, which was equivalent to 222,856-251,415 events per day. Although the number of cybersecurity events decreased to 53 million in 2015, the number of security incidents (which are regarded as the most serious cyber-attack classification) was up 64% from the 109 that were discovered in 2014 (see exhibit 19). The global cost of digital crimes and IP thefts amounted to USD575.0bn in 2015, according to the US-based Centre for Strategic and International Studies (CSIS). Moreover, the cost of cybercrime is expected to escalate as an increasing number of functions including, business operations to customer-retailer interactions, move online. Hence, Juniper Research predicts that the magnitude of information security losses would grow by a factor of 4x to USD2.1tn by 2019, despite billions invested in cybersecurity.

Exhibit 19: Average annual cybersecurity events, attacks and incidents



Event: An event on a system or network detected by a security device or application.
Attack: An event identified as malicious activity attempts to collect, disrupt, or destroy information
Incidents: An event reviewed by IBM security analysts and deemed worthy of deeper investigation
Source: IBM

According to PwC's Global State of Information Security Survey, in 2015, 38% more security incidents were detected than in 2014. According to the Identity Theft Resource Center, the majority of cyber attacks' victims in 2015 were healthcare and government sectors, which accounts for 66.7% and 20.2% of total incidents, respectively. The table below provides notable cybersecurity breaches in 2015.

Exhibit 20: Notable 2015 Cybersecurity Breaches

	Target	# Persons affected	Notable Aspects
Jan	Premera Blue Cross	11.0mn	Initial attack dated back to May 2014; FireEye hired to investigate with FBI
Feb	Anthem	78.8mn	Largest healthcare data breach to date
Jun	Ashley Madison	37.0mn	Company charging users for what they claimed were "full delete" services
Jun	Office of Personal Management	21.5mn (US only)	Victims were mainly military and government personnel
Aug	Excellus Blue Cross Blue Shield	10.0mn	Third largest healthcare breach of 2015; revealing sensitive data of approximately 80 million individuals
Sep	Experian / T-Mobile	15.0mn	Victims were new T-Mobile customers, who underwent a credit check from 9/1/13 - 9/16/15
Nov	VTech Holdings Ltd	11.3mn	6.9 million child accounts and 4.9 million parent accounts breached

Source: MicroMarketMonitor

Given the increasing and more sophisticated cyber attacks, we expect businesses of all sizes and types, and governments globally to concentrate on cyber protection. Gartner stated that the worldwide IT security market was valued around USD75.4bn in 2015, representing an increase of 4.7% over 2014. The firm also expects the global cybersecurity market to grow at a Compound Annual Growth Rate (CAGR) of approximately 8.1% through 2020 with stable demand across security technologies and services. According to another report published by MarketsandMarkets, the sector is estimated to grow at a CAGR of 9.8% to USD170.0bn over the same period. The aerospace, defense and intelligence verticals are expected to be the largest contributors to cybersecurity solutions.

Regarding the revenue breakdown by region, MicroMarketMonitor reported that the Europe Cybersecurity Market is expected to grow up to USD35.5bn by 2019, with an expected CAGR of 7.2% for the period 2014-2019. For the same period, cybersecurity markets in the US and Asia-Pacific region are expected to reach USD72.1bn and USD33.0bn, respectively (see Exhibit 21). Hence, the picture for cybersecurity market is a bit more promising.

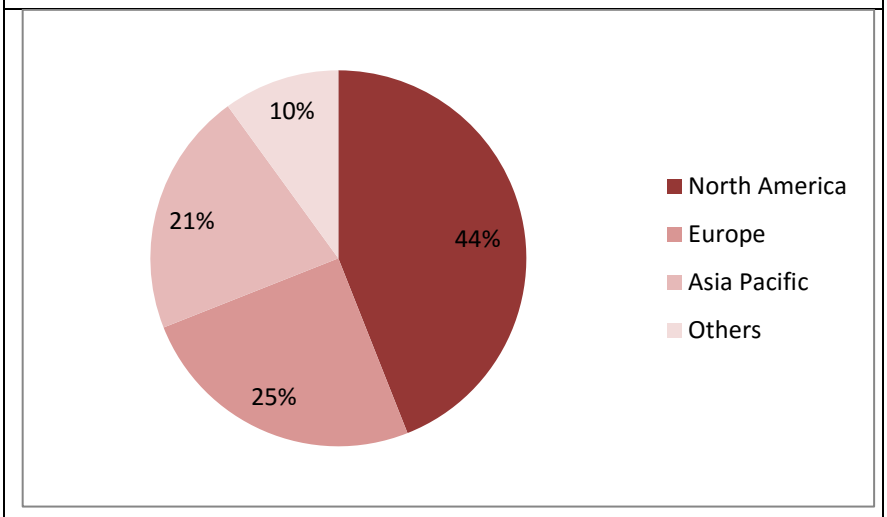
Exhibit 21: Projected cybersecurity market growth by region (2014-2019)

Region	USDbn	5-year CAGR	2014 market share
United States	72.1	7.3%	43.4%
Europe	35.5	7.2%	27.0%
MEA	13.4	13.7%	7.2%
Asia Pacific	33.0	14.1%	17.2%
Latin America	11.9	17.6%	5.2%
	165.9	**9.9%**	

Source: MicroMarketMonitor

North America continues to dominate spending in IT Security, accounting for over 44% of worldwide revenues in 2015, while Western Europe accounts for over 25% and Asia Pacific, including China, over 21%. Together these three regions make up more than 90% of the global spend (see Exhibit 22 below). Moreover, North America and Europe are forecast to continue being the leading contributors of the sector's total revenues whereas Asia-Pacific countries, largely driven by emerging markets like China and India, are expected to become potential markets for security solutions, according to a report from TechSci Research.

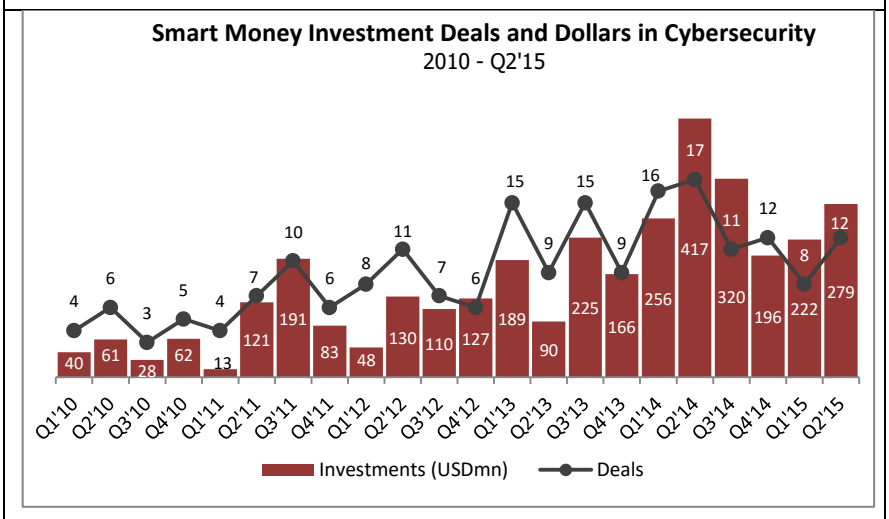
Exhibit 22: Global IT Security Spending 2015: Geographical Contribution



Source: IDC

As investors have realized the potential growth in the IT security market, investments in sector-related startups, especially cybersecurity companies, have increased. Investment tracking firm CB Insights reported that overall funding in the cybersecurity market reached USD1.2bn in 2014 or about six times the 2010 figure (see Exhibit 23 below). Moreover, according to US-based investment banking FBR & Co, the number of seven-figure cybersecurity deals has increased by 40 percent y-o-y.

Exhibit 23: Smart Money Investment Deals and Dollars in Cybersecurity



Source: CB Insights

Company Focus - Cybersecurity Market

The cybersecurity market is marked by the presence of several established players such as IBM, Check Point Software Technology, Intel, Cisco, Sophos, Trend Micro, Lockheed Martin and Symantec. However, WISeKey's more direct competitors are primarily companies which focus on protecting online communications and data for consumers, organizations and servers. They include RSA, Symantec, DigiSign, CyberTrust, FireEye and Iron Mountain. As mentioned earlier, MarketsandMarkets reported that the global cybersecurity market is expected to grow from USD106.3bn in 2015 to USD170.2bn by 2020. A substantial driver is the rising number of companies detecting cyber attacks with significant monetary damages, growing online and mobile transactions, increasing internet-connected devices. Moreover, North America is expected to become the largest market in terms of spending and adopting cybersecurity solutions. Given WISeKey's recent expansion with its first office in the US, the company is able to explore more opportunities in this sector.

Company Focus – IoT / DBM Market

The IoT security market is expected to grow from USD655.8bn in 2014 to USD1.7tn in 2020 which represents 17.2% CAGR of over the six-year period, according to a report released by research firm IDC. In addition, the number of connected devices requiring digital identification and security now tops 4 billion globally and is expected to increase substantially by 2020, which indicates a major potential transformation. The IoT/DBM market includes several well-known companies such as Bastille, Corporation Service Company, VeriSign and Symantec. However, according to WISeKey management, the company currently does not face direct competition from companies providing brand management products for digital authentication of luxury watches, high-end glasses, smart phones and designer clothes. Given the fact that advanced counterfeiting continues to challenge organizations, WISeKey wants to further expand this business and increase its DBM product family sales to luxury product manufacturers.

Company Focus – Mobile Security Market

MarketsandMarkets predicts the global Mobile Security market to increase from USD1.5bn in 2014 to USD5.8bn by 2019, representing a CAGR of 30.7%. There are currently many companies providing Mobile Security products including Kaspersky, Sophos, Symantec Corporation, McAfee and Trend Micro. However, WISeKey's direct competitors are limited to those offering personal data-secured and Customer Relationship Management (CRM) products which, generally, fall under Identity and Access Management (IAM) market. According to a research by MarketsandMarkets, the IAM market is expected to grow from USD7.2bn in 2015 to USD12.8bn by 2020, representing a CAGR of 12.2% during the five-year period. Moreover, North America was the largest revenue generator of this market sector in 2015. Among the major players in the IAM space are IBM, Oracle, Microsoft, Intel, Okta, and SailPoint. However, more direct competitors to the company are Good Technologies, PasswordBox and Mobile Iron.

We have compiled the following list of companies, which manufacture various products similar to WISeKey's.

Exhibit 24: WISeKey – Comparison with Industry peers

Cybersecurity Services	IoT/DBM	Mobile Security
Symantec	Corporation Service Com.	Good Technologies
DigiSign	VeriSign	PasswordBox
FireEye	Symantec	Mobile Iron
CyberTrust	Bastille	IBM
Iron Mountain		Microsoft
RSA		Intel
Trend Micro		Oracle
IBM		Okta

Source: Company data, press release

GROWTH OPPORTUNITIES & KEY DRIVERS

Cyber attacks widely acknowledged as a major threat, inducing a need for cybersecurity

As mentioned earlier, the global cost of digital crime and IP theft amounted to USD575.0bn in 2015. The cyber crime costs did quadruple in the period between 2013 and 2015 and are expected to have another quadrupling from 2015 to 2019. According to Juniper's recent research, the cost of data breaches will amount to USD2.1tn globally by 2019, corroborating the fact that cyber crimes have become the greatest threat to every company in the world. Moreover, there is a growing demand for securing IoT devices, which are expected to reach 28 billion in 2021, according to the 2016 Ericcson Mobility Report (see Exhibit 25). This creates favorable market backdrop for WISeKey's long-term growth in the market.

Exhibit 25: The IoT connected devices (in billions)

	2015	2021	CAGR 2015-2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%
	15 billion	**28 billion**	

Source: 2016 Ericcson Mobility Report

According to a report from Gartner, over a quarter of identified cybersecurity attacks in enterprises are predicted to involve IoT by 2020. Furthermore, the research company forecasts that worldwide IoT spending would reach approximately USD550.0mn by the end of 2018, representing an almost hundred percent increase from 2015 spending of USD281.5mn (see Exhibit 26).

Exhibit 26: Worldwide IoT Security Spending Forecast (Millions of Dollars)

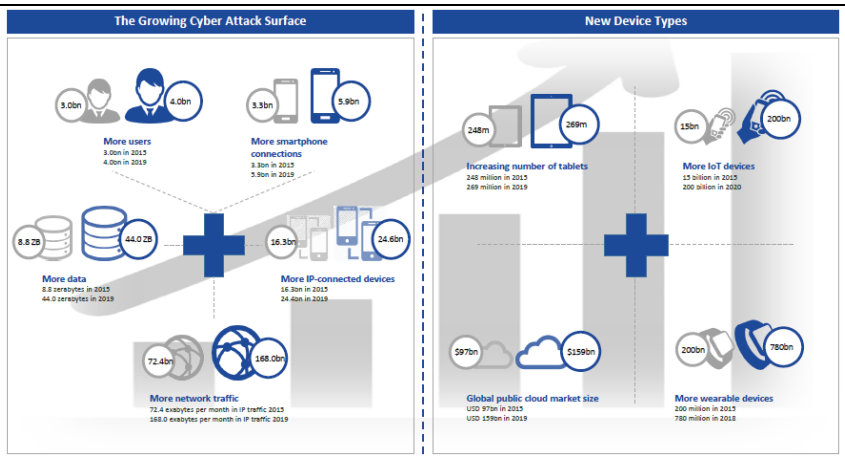
2014	2015	2016	2017	2018
231.86	281.54	348.32	433.95	547.20

Source: Gartner

WISeKey has already been involved in cybersecurity solutions long before recent developments in cyber threats. WISeKey's key technology cryptographic RoT, which is being protected by Switzerland's political, financial and regulatory stability, has been used since 1999 by over 2.6 billion desktops, browsers, mobile devices and other IoT devices. Being able to benefit from geopolitical advantage, WISeKey makes its RoT technology available to IoT manufacturers and chipmakers globally, allowing them to add digital certificates on their chips at the hardware level.

Moreover, recent customer identity thefts affecting prominent consumer brands highlight the hazards of personal data exposure. Data attackers utilize the gap between a person and an authenticated process to steal consumer identity and related data. WISeKey's WISeID can protect users against this threat by protecting users' personally identifiable information (PII) and its associated content. WISeID provides users with a secure encrypted place from bunkers in the Swiss Alps to store all personal data, PII, usernames, passwords, PINs, credit cards, and more. As there are no international regulations on how to protect consumers, Swiss neutrality is a key asset in ensuring data for consumers, enterprises and governments.

Exhibit 27: Opportunity due to growing cyber attack surface



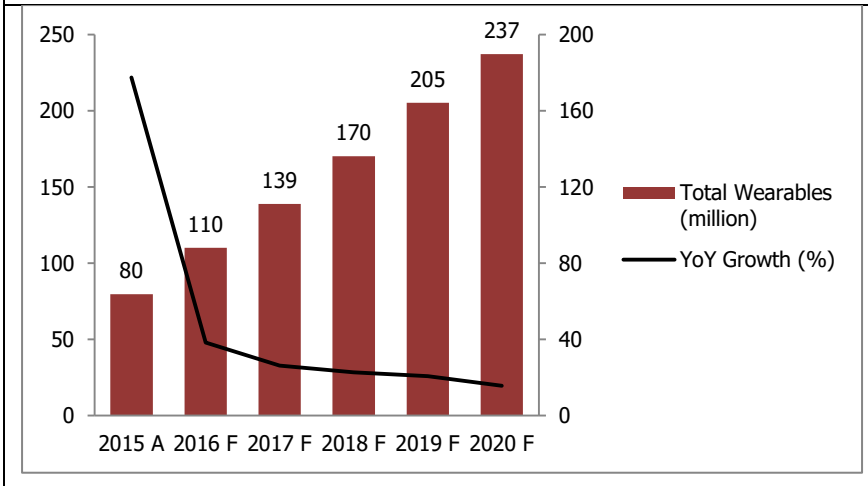
Source: WISeKey's Annual Report 2015

Evolution of WISeKey's technology creating growth opportunities in IoT market

In 2015, the company announced co-operations with Bulgari, Hublot, Kaspersky Labs and Samsung to implement WISeKey's IoT technology, which is used to identify watches electronically and prevent counterfeiting products. Today, over one million watches are digitally tagged by the company. The figure is expected to significantly increase, especially after the company's recent partnership with MasterCard that allows payments by using luxury branded watches or wearable devices. The rapid growth of connected devices is driving a shift from traditional payment methods to more secure and reliable ones using trusted communications and authentication technology. Therefore, the potential for improved customer satisfaction from providing them more options to securely using connected fashionable and functional accessories creates a strong base for company growth in this business.

WISeKey and Bulgari launched the first intelligent watch in 2015 which allows the watch to execute payment transactions without using a mobile phone or other connected device. The company claims that this breakthrough in innovation provides WISeKey an opportunity to have its technologies embedded in all wearables with an estimated market value of USD1.7tn. According to the IDC, worldwide shipments of wearable devices are expected to reach 110 million in 2016 and may go up to 237.1 million in 2020 (see Exhibit 28). Watch and wristband shipments would hover around 100 million for 2016. Therefore, the company's expectation of impressive growth in this sector is well-justified. Moreover, the company believes that the global wearable market would grow at an annual rate of 35% over the next five years.

Exhibit 28: Worldwide Wearables Shipments Forecast



Source: IDC

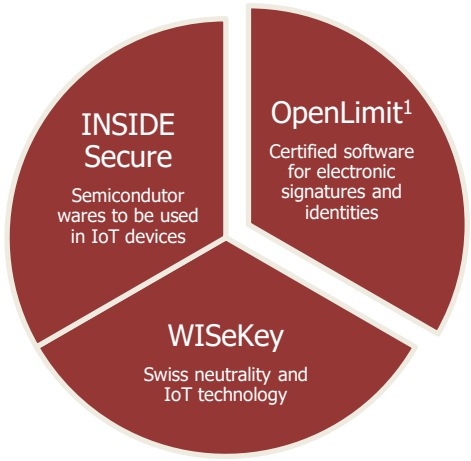
WISeKey's revenue is mainly contributed by cybersecurity IoT sales, which is an entirely new revenue model introduced by the group in 2014/2015. Given the promising outlook for IoT business segment, the company's performance is expected to be in the positive territory.

Expanding through accretive acquisitions

WISeKey has recently pursued additional add-on acquisitions to consolidate its position as a comprehensive cybersecurity player. These strategic mergers enable the company to fully focus on the rapidly expanding cybersecurity market and provide WISeKey an opportunity to cash in on a burgeoning demand for IoT devices.

WISeKey recently acquired the semiconductor assets of INSIDE Secure, a France-based provider of embedded security solutions. Adding INSIDE Secure's offerings enables WISeKey's cryptographic RoT to add digital certificates on the integrated circuits designed by the company at the hardware level to encrypt communication and authenticate the devices. This allows WISeKey to have a comprehensive cybersecurity trusted platform with complete vertical integration in combining hardware, cryptography and software. More importantly, the combination reinforces WISeKey's position as a cybersecurity IoT player with strong potential in an emerging IoT environment which remains ripe for potential cyber attacks. This further consolidates our previously-mentioned view on WISeKey's performance within IoT market. Therefore, we expect that a major increase in the company's FY2016 sales will result directly from this consolidation.

Exhibit 29: Strategic acquisitions offer broad potential for WISeKey to grow in the IoT market



Source: Company Analysis
Note:
1. WISeKey has only signed an MoU to merge with OpenLimit

Additionally, WISeKey has recently signed an MoU with OpenLimit Holding AG regarding a proposed business combination via a statutory merger, whereby OpenLimit would be merged with and into WISeKey. The combined product and service portfolios of WISeKey and OpenLimit will enable the group to provide more comprehensive solutions from "chip-to-root" to its customers. Moreover, the combination will also give WISeKey an access to OpenLimit's customers in Germany and other mature markets in Europe. This coupled with the WISeKey's recent move to establish a new office in the Silicon Valley indicates that the Company is trying to further consolidate its footprints as a global cybersecurity company.

Promising outlook for the IoT market

Going forward, we expect WISeKey to continue to pursue vertical acquisitions to complement its current product offerings and eventually become a comprehensive provider of cybersecurity and IoT solutions. Even though there has been a slow but continual development of the IoT sector since the early 2000s, the market is expected to rapidly expand in the coming years given the rising concerns about cybersecurity threats. Therefore, further consolidations would enable the company to capture market share and strategically position itself among other competitors. However, other players are also following the trend. One such deal involved two Czech-originated companies Avast Software and AVG Software. The merger, wherein Avast Software will acquire AVG Technologies, will put the combined entity in a better position to take advantage of new growth opportunities in the IoT space.

According to a study released by Strategy Analytics in April 2016, there have been nearly 24 major IoT-related mergers and acquisitions in the first four months of 2016. According to the report, the most desirable acquisition targets are companies whose core competencies revolve around analytics, security, connectivity platform capabilities and services. In 2016 alone, tech giants such as Intel, Microsoft and Cisco have spent extravagantly on acquisitions to boost their IoT portfolios. Mentioned below are some of these acquisitions.

Exhibit 30: Major IoT acquisitions in 2016

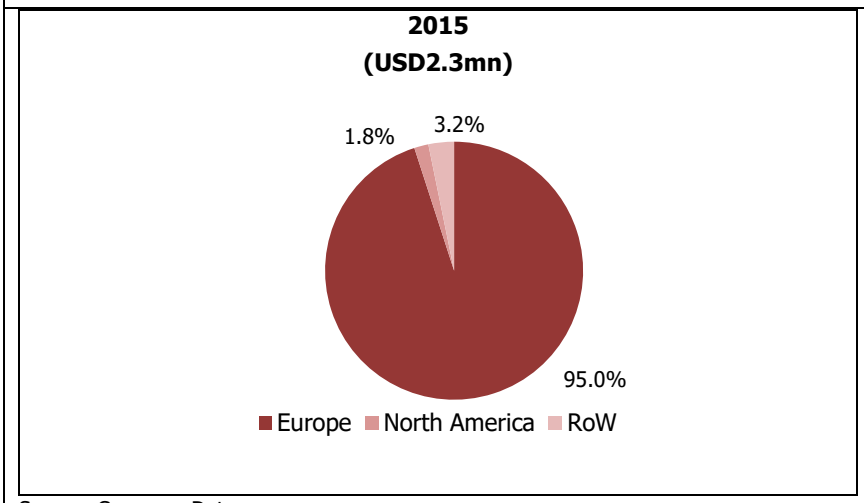
Date	Acquirer	Target	Deal Value (USDmn)
Jan-16	Sony Corp.	Altair Semiconductor	212
Feb-16	Cisco	Jasper Technologies	1,400
Apr-16	Brocade Communications	Ruckus Wireless	1,225
Apr-16	Nokia	Withings	n.a.
Apr-16	Intel	Yogitech	n.a.
Apr-16	Qorvo	GreenPeak Technologies	n.a.
May-16	ARM	Apical Ltd.	350
May-16	Microsoft	Solair	n.a.
Jun-16	Cypress Semiconductor Corp.	Broadcom's Wireless IoT Business	550

Source: Strategy Analytics Report April, 2016

More expanding opportunities in the US market

The Exhibit 31 provides key insights into WISeKey's revenue breakdown by region. Most of the company revenues currently come from European countries, including Switzerland. Only 1.8% of its revenue is derived directly from the US in 2015. Hence, there is room for expansion in the US market. WISeKey's revenues for FY2015 were USD2.3mn as compared to USD3.5mn for FY2014. FY2015 was a transitional year for the company due to reorganization of the whole group and the strategic repositioning towards a listing on the Swiss market. Also, majority of the revenue contribution was from cybersecurity IoT sales, which is a new revenue model introduced by the Group in 2014/15. We believe that it would take WISeKey some time before this new model reflects substantial y-o-y revenue growth.

Exhibit 31: Revenue Breakdown by Region



Source: Company Data

In 2015, the company established its first office in Silicon Valley in order to be closer to US target customers. WISeKey's definitive agreement with US-based CenturyLink allows the US company to resell WISeKey's portfolio of cybersecurity solutions to serve a growing number of cyber safety demands from the government, enterprises and IoT customers. According to a report from Home Land Security Research, the US financial institutions cybersecurity market is expected to be the largest and fastest growing private sector, with a cumulative 2016-2020 size forecasted to exceed USD68.0bn. Moreover, the US government budget allocated to cybersecurity has increased by 35% from USD14.0bn in 2016 to USD19.0bn in 2017, as stated by President Barack Obama over the IT security issue. Therefore, WISeKey expects this collaboration with CenturyLink to start contributing significant revenue from the North American region in 2017 and expanding its geographical market share. Moreover, current established channel partnerships with Samsung, Microsoft, HP, SAP and others would also promote aggressive US expansion in coming years.

Exhibit 32: Federal Agency Incidents Reported to US-CERT

Reporting Source	FY 2013 Reported Incidents	FY 2014 Reported Incidents	FY 2015 Reported Incidents
CFO Act Agencies	57,971	67,196	75,087
Non-CFO Act Agencies	2,782	2,655	2,096
Total Federal Incidents	**60,753**	**69,851**	**77,183**

Source: Data reported to US-CERT Incident Reporting System from Oct 1, 2012 to Sep 30, 2015.

In short, after several years of investing a significant amount of resources, the company now starts to monetize growing opportunities. With its cryptographic RoT, the company has created a crypto- and software-based platform which is compatible with a wide range of internet and mobile applications and operating systems. WISeKey provides tailored solutions to address the key issues faced by government, corporate and retail customers in the field of cybersecurity, identification and authentication management.

KEY RISKS

Significant competition

The company faces regular competition with respect to innovation and evolving security threats in the digital security market. Several global security companies, including VeriSign Inc., Symantec Corporation, FireEye Inc., Red Hat Software, VASCO Data Security International Inc. and Zix Corp, with large technical and financial resources and broad customer bases, are some of the players which operate in the same space as the company.

Such companies may use these advantages to offer products and services that are perceived to be as effective as the company's at a lower price or for free as part of a larger product package or solely in consideration for maintenance and services fees. They may also develop different products to compete with the company's current solutions and respond more quickly and effectively than the company to new or changing opportunities, technologies, standards or client requirements.

High sales concentration on small business and dependence on a few industries that could be afftected by economic downturn

In 2015, one of company's customers in the luxury watch business accounted for 53% and two costumers for 17% each of its revenues. The company plans to broaden its customer base but expects that a limited number of customers will continue to account for a substantial portion of revenues for the foreseeable future. The company may be negatively affected as a result of loss of any of these customers.

The company also expects to generate a significant portion of its revenues from manufacturers of luxury goods, which generally suffer more dramatically during a time of economic downturn. Negative economic conditions may cause such customers to reduce their spending, including for security applications. Customers may delay or cancel projects, choose to focus on in-house development efforts or seek to lower their costs by renegotiating service agreements with us. All these possibiities may negatively affect company's operations.

History of losses and lack of profitability

So far, the company has invested over CHF105.0mn in its brand technology and market position. It has not been profitable since its inception and had an accumulated cumulative loss of USD119.7mn for FY15. WISeKey also expects to make significant future investments to support further development and expansion of its business. These investments may not result in increased revenue or growth on a timely basis or at all.

Termination of the license agreement with OISTE

OISTE has granted WISeKey a perpetual license to use the cryptographic rootkey technology and develop technologies & processes based on OISTE's trust model. The license agreement which can only be terminated under limited circumstances, including if the company were to move from the trust model developed by OISTE or changing the location of the RoT from Switzerland to another country, can present a significant threat to the company's current trust model.

Exposure to foreign exchange risks

The company's reporting currency is the US dollar while it generates most of its revenues in the Swiss franc. In 2014, most of its revenues were denominated in Swiss francs and the remainder primarily in US dollars and the Euro. In 2014, a substantial majority of the cost of revenues and operating expenses were also denominated in the Swiss franc and the remainder primarily in the Euro.

As the company is expanding in the US market, it expects to generate additional revenue in US dollars and other currencies. The company estimates that a 10% increase or decrease in the value of the Swiss franc against the US dollar would have decreased or increased the net loss by approx. USD481,000 and USD529,000 respectively, in 2014.

Potential software errors may affect company's business

WISeKey offers complex software applications which are subject to risks related to defects or errors, especially where updated versions of the software or any enhancements are released. This could negatively impact the company's business, including lost revenue, a delay in market acceptance or a customer claim.

VALUATION

Given WISeKey's niche business profile, there are not many exact comparables available. In order to show relative valuation of the group, we have prepared a customized set of peers whose end-markets are similar to that of WISeKey. The companies considered include Netherlands-based NXP Semiconductors NV (NXP), Netherlands-based Gemalto NV (Gemalto), Norway-based Idex ASA (Idex) and US-based salesforce.com, Inc, among others. The list of the peers has been obtained from S&P Capital IQ and the information provided in the company documents.

We have considered the three most widely used parameters, EV/Revenue, EV/EBITDA and P/E to show relative valuation of the group. Our exhibition as depicted in the below table highlights that on a 2-year forward multiples WISeKey is trading at only a slight discount of 7.1% on EV/Revenue and on a premium of 208.7% on EV/EBITDA, and 99.7% on P/E multiple compared to its industry peers. We believe this is mainly due to the aggressive growth strategies followed by the group, especially in the past year in terms of restructuring and listing on the Swiss Stock Exchange in 2016. Also, WISeKey is on the verge of embarking on its growth story as it has started to vertically integrate its product offerings via recent acquisitions including INSIDE Secure and the impending merger with OpenLimit. Additionally, the strategic partnerships with major global players such as SAP, Microsoft, MasterCard and CenturyLink, should ensure that WISeKey will be able to monetise on the synergistic opportunities created by offering chip-to-root solutions to its customers.

Exhibit 33: WISeKey – Comparison with Industry peers

Company Name	EV/Revenue			EV/EBITDA			P/E		
	2015A	2016E	2017E	2015A	2016E	2017E	2015A	2016E	2017E
WISeKey International Holding Ltd	NM	16.4x	4.8x	NM	NM	33.1x	NM	NM	36.1x
NXP Semiconductors NV	6.1x	3.9x	3.8x	20.4x	10.1x	9.6x	19.4x	NM	23.3x
Idex ASA	NM	NM	5.1x	NA	NM	NM	NM	NM	NM
Juniper Networks, Inc.	1.8x	1.8x	1.7x	6.7x	6.9x	6.4x	14.1x	16.7x	14.6x
Red Hat, Inc.	7.1x	6.2x	5.3x	27.1x	22.9x	19.6x	NM	NM	NM
Palo Alto Networks, Inc.	12.5x	8.5x	6.3x	NM	NM	27.4x	NM	NM	NM
VeriSign, Inc.	7.6x	7.1x	6.9x	11.3x	10.2x	10.0x	21.6x	19.0x	18.3x
FireEye, Inc.	3.7x	3.2x	2.7x	NM	NM	NM	NM	NM	NM
Check Point Software Technologies L	7.1x	6.7x	6.3x	12.4x	12.2x	11.5x	18.8x	18.7x	17.9x
Average	6.6x	5.3x	4.8x	15.6x	12.5x	14.1x	18.5x	18.1x	18.5x
Median	7.1x	6.2x	5.2x	12.4x	10.2x	10.7x	19.1x	18.7x	18.1x
High	12.5x	8.5x	6.9x	27.1x	22.9x	27.4x	21.6x	19.0x	23.3x
Low	1.8x	1.8x	1.7x	6.7x	6.9x	6.4x	14.1x	16.7x	14.6x
Premium (disc) to product peers	NM	165.8%	(7.1%)	NM	NM	208.7%	NM	NM	99.7%

Source: S&P Capital IQ and Research Dynamics

Using discounted cash flow (DCF) methodology, the intrinsic price of the group comes to CHF14.9. Our weighted average cost of capital (WACC) of 13.6% is based on a cost of equity of 13.6% and cost of debt as *nil* since the company does not have any debt in its balance sheet. Our inputs for cost of equity include beta of 1.20 (time span: last five years), current 10 year government bond yield of 2.6% and long term average return of 5.8% generated by the Swiss Market Index. Our assumptions are based on aggressive growth plans; we have explicitly forecasted cash flows till FY2021E and thereafter assumed a terminal growth rate of 3.0%.

Exhibit 34: Sensitivity of WACC and Terminal Growth

Enterprise Value Sensitivity					
	Terminal Growth Rate				
WACC	1.5%	2.0%	2.5%	3.0%	3.5%
11.6%	527	550	575	603	635
12.6%	467	485	505	527	551
13.6%	418	432	448	465	484
14.6%	376	388	400	414	429
15.6%	341	350	361	372	384

Source: Research Dynamics

Exhibit 35: Sensitivity of WACC and Implied Multiple

Implied Multiple EV / 2017 Revenue					
	Terminal Growth Rate				
WACC	1.5%	2.0%	2.5%	3.0%	3.5%
11.6%	5.5x	5.7x	6.0x	6.3x	6.6x
12.6%	4.9x	5.1x	5.3x	5.5x	5.7x
13.6%	4.4x	4.5x	4.7x	4.9x	5.0x
14.6%	3.9x	4.0x	4.2x	4.3x	4.5x
15.6%	3.6x	3.7x	3.8x	3.9x	4.0x

Source: Research Dynamics

FINANCIALS (HISTORICALS AND KEY FORECASTS)

Revenue

WISeKey's performance trend has been volatile especially in the past couple of years. Revenues for FY2015 were USD2.3mn as compared to USD3.5mn for FY2014. The fall in revenue was attributable mainly to the European region (down by 33.6% y-o-y, c.95% of revenue) and North America (down by 67.4%). Against this, revenue marginally went up in the RoW segment (up by 4.8%). But this increase was not sufficient to offset the fall in the other two big geographical segments. The majority of the revenue contribution was from cybersecurity IoT sales, which is a new revenue model introduced by the Group in 2014/15. The operating loss, however, substantially decreased from USD32.4mn in 2014 to USD7.5mn in 2015.

However, the future looks promising as the company is on its way to become a vertically integrated cybersecurity platform providing chip-to-root solutions to the customers. The company plans to achieve this by making strategic acquisitions in various verticals and being able to cross-sell its wide range of product offerings. Going forward, we have modeled sales to grow exponentially in FY2016e and FY2017e to arrive at figures of CHF28.0mn and CHF96.0mn, respectively. To arrive at this number, we have assumed growth rates for the company's recent acquisition (INSIDE Secure) and potential acquisitions currently under discussions. We have also taken into consideration the company's strategic partnerships with SAP. Additionally, we have applied a growth rate to company's WISeID service.

These acquisitions and partnerships create a synergistic product platform wherein the company can cross-sell the solutions across any of these verticals. We believe, this business model possesses huge potential in terms of generating revenues in the coming years. Hence, we have considered significant growth rate assumptions especially with respect to company's partnership with industry-leading SAP HANA cloud platform. Since SAP's HANA platform has already gained wide industry acceptance, we opine WISeKey could grow its revenue share substantially.

Earnings before interest, tax, depreciation and amortization (EBITDA)

WISeKey's EBITDA has been in the negative bracket historically as the company was not earning substantial revenues. But similar to its top-line, profitability is expected to increase in the near future. The same is expected to rise to CHF14.0mn for FY2017e and increase further up to CHF85.0mn in 2021e representing a CAGR of 57.1%.

Again, we expect the EBITDA growth to remain robust on the back of solid partnerships with major global companies, which would enable WISeKey to become an end-to-end provider of cybersecurity solutions.

ADDITIONAL DETAILS

WISeKey's management and Board of Directors comprise industry experts with proven credentials in the cybersecurity industry.

Key Management team

Carlos Moreira
Founder, Chairman and Chief Executive Officer

Mr. Moreira started his career as a UN expert on IT, eSecurity and Trust Models, working for ILO, UN, UNCTAD, ITC/WTO, World Bank, UNDP, ESCAP from 1983 to 1998. He founded WISeKey in 1999. He has also founded various forums including Geneva Security Forum and Geneva Philanthropy Forum. Mr. Moreira has also held and holds various positions of responsibility in various global organizations, including the UN Global Compact, World Economic Forum's Global Agenda Council.

Peter Ward
Chief Financial Officer

Mr. Ward began his tenure with WISeKey SA in 2008 as the Finance Director and has been the Chief Financial Officer and a Board member since 2012.

He has experience in the IT, FMCG, Retail/Distribution, Medical Equipment and Plastics industries, having worked in companies such as ITT, General Electric and Iomega. He has experience in Change Management, Process Improvement, Business Integration & Restructuring as well as extensive knowledge of International Tax, Statutory and US GAAP reporting and Sarbanes-Oxley requirements. Mr. Ward is a Chartered Management Accountant and holds a BA (Hons) degree in Business Administration from Wolverhampton University, U.K.

Carlos Moreno
VP, Digital Brand Management

Mr. Moreno has over 18 years' experience in sales engineering, sales management and business development. He has held executive roles in the areas of people management, sales coaching, market analysis, establishment and implementation of account plans. In his role in WISeKey, he oversees commercial relationships with strategic customers and serves as the head for market analysis and go-to-market strategies. He has also contributed to the design of solutions and architectures in projects related to infrastructure, data, applications, security and dentity management and overall evolution of WISekey's product suite.

Pedro Fuentes
Chief Information Security Officer & VP Cybersecurity Solutions

Mr. Fuentes obtained a high degree in Computer Science by the Polytechnic University of Valencia and he's a senior specialist in information security, and PKI in particular, with more than 20 years of active work in these areas as a certified professional (CISM, ISO27000, MSCP and others). Pedro joined WISeKey in 2009 to reinforce the eSecurity Business Unit. Previously he worked in Siemens as responsible of the cybersecurity product line for southern Europe. In WISeKey Mr. Fuentes is responsible for the PKI platforms and product strategy, leading projects and customer support worldwide.

Elie Massabki
WISeKey USA SVP Sales Marketing

Mr. Massabki has 25 years of experience in general management, sales, marketing, business development and engineering. Prior to joining WISeKey, he led Kili Technology's sales and marketing efforts globally and established Kili's US office in Silicon Valley. Kili was later sold to mobile payment company Square Inc. Prior to Kili, he worked with companies such as Syfx Tekworks, ChipX, GigOptix, Conexant, Mindspeed and IDT. Mr. Massabki a B.S.E.E and a M.B.A. from Santa Clara University.

Youmna Abisaleh
WISeKey Marketing and Communication

Ms. Abisaleh started her career in marketing with two FMCG companies, Heineken and L'Oreal. Youmna graduated from HEC Geneva in 2012 with a master's degree in Strategic Marketing and Management and completed her studies with two Erasmus in the Dauphine University in Paris and the Humboldt University in Berlin. Ms. Abisaleh has been involved in developing creative tools in digital marketing and helped brands to improve their online campaign.

Board of Directors

Carlos Moreira
Chairman

Peter Ward
Director

Dourgam Kummer
Director

Mr. Kummer joined WISeKey SA in 2005 as the CFO. He has held several leading positions in the structure and corporate finance in international companies and financial institutions including André & Cie SA. He graduated in Company Management and Finance at "l'école de Cadre" in 1988 in Lausanne and obtained a degree on Structure Finance in 1998 and in Strategic Finance in 2006 at IMD.

Philippe Doubre
Director

Mr. Doubre is currently a member of the board of the WTCA in New York and is a former Chairman of the WTCA Committee on Information and Communication. He also serves as the President of the China Hub in Geneva and a permanent representative of the WTCA organizations to the UN in Geneva. He is also a President of the OISTE Foundation. Prior to this position, Mr. Doubre held several senior positions in the banking and finance industry.

Dr. Franz Humer
Director

Dr. Humer is currently also Chairman of the Board of Directors of the International Centre for Missing and Exploited Children and the Humer Foundation. He is an independent director with Citigroup Inc., Chugai Pharmaceuticals Ltd (Japan), Bial Pharmaceuticals (Portugal), Kite Pharma (a biotech company in Los Angeles) and a member of the International Advisory Board of Allianz SE.

Dr. Humer has also worked with companies such as Schering Plough, Glaxo Holdings, Roche and Diageo. He has obtained a PhD in Law from Innsbruck University and an MBA from INSEAD in Fontainebleau.

Juan Hernandez Zayas
Director

Mr. Zayas currently serves as a member of the ROAC (The official Spanish College of Chartered Accountants). In recent years, he has also been focused on leading development in several new tech and renewable energy entities. Mr. Zayas has worked as the CEO of the Cosimet-Velasco Group (joined in 2001), where he played a major role in the Company's diversification strategy and in the consolidation of a large industrial holding. He graduated in Economics and Business Administration in Bilbao in 1987, and obtained an MBO at the LSFT (London).

Maryla Shingler Bobbio
Director

Ms. Shingler currently serves as the founder and Managing Director of the Argentum Group. She has worked in various law firms in London including Linklaters, Beachcrofts and Charles Russell. She has also worked with Rathbones plc. Maryla is a full Member of the Society of Trust and Estate Practitioners (STEP) and holds a current English Solicitor Practising Certificate.

Thomas Egger
Director

Mr. Egger currently works with Parkview Ltd. (since June 1, 2012), as its CEO/Adviser. He began his career in 1976 with an apprenticeship/Business School at Swiss Bank Corporation (predecessor to UBS AG) where he was until recently serving in the position of Senior Advisor/Managing Director, UBS Wealth Management for Latin America and the Iberian Peninsula. From 1999 - 2003, Mr. Egger led the global UBS Sports & Entertainment initiative.

DETAILED FINANCIAL STATEMENTS

Income Statement

Figures in CHF'mn	2014A	2015A	2016E	2017E	2018E	2019E	2020E	2021E
Total revenue	3.3	2.2	28.0	95.8	123.1	149.6	177.3	206.0
COGS	(1.3)	(0.8)	(10.6)	(34.9)	(40.0)	(42.8)	(44.2)	(44.1)
Gross profit	2.0	1.4	17.4	61.0	83.1	106.7	133.1	161.9
Research and development	(2.0)	(0.6)	(5.5)	(11.8)	(13.6)	(16.0)	(17.8)	(19.2)
General and administrative	(14.2)	(4.3)	(8.7)	(18.8)	(21.7)	(25.6)	(28.4)	(30.8)
Sales and marketing	(17.3)	(1.3)	(7.6)	(16.5)	(19.0)	(22.4)	(24.9)	(26.9)
Loss on impairment	-	(1.5)	-	-	-	-	-	-
Total operating Costs	(33.5)	(7.8)	(21.9)	(47.0)	(54.3)	(63.9)	(71.1)	(77.0)
EBITDA	**(31.5)**	**(6.3)**	**(4.4)**	**13.9**	**28.8**	**42.8**	**62.0**	**84.9**
Depreciation	0.1	0.0	0.3	1.0	1.2	1.5	1.8	2.1
Amortization	0.6	0.3	0.0	0.0	0.0	0.0	0.0	-
Operating Profit (EBIT)	**(32.1)**	**(6.6)**	**(4.7)**	**13.0**	**27.5**	**41.3**	**60.2**	**82.8**
Interest income	0.0	0.0	0.0	0.1	0.4	0.7	1.1	1.6
Interest expenses	(0.0)	(0.0)	-	-	-	-	-	-
Other income (expenses), net	(0.1)	0.2	0.1	0.3	0.4	0.4	0.5	0.6
Loss on investments in associated companies	(0.1)	(0.0)	-	-	-	-	-	-
Income before taxes	**(31.7)**	**(6.2)**	**(4.6)**	**13.4**	**28.3**	**42.5**	**61.8**	**85.0**
Income taxes	(0.0)	(0.0)	-	-	-	-	(3.8)	(16.2)
Net income	**(31.7)**	**(6.2)**	**(4.6)**	**13.4**	**28.3**	**42.5**	**8.0**	**68.8**

Source: Research Dynamics

Balance Sheet

Figures in CHF'mn	2014A	2015A	2016E	2017E	2018E	2019E	2020E	2021E
Cash and cash equivalents	0.0	0.4	0.5	0.4	14.4	41.8	67.6	105.0
Trade receivables, net of allowances for doubtful accounts	0.2	0.1	0.2	0.3	2.3	7.8	10.0	12.1
Receivables from shareholders	0.6	0.0	0.1	0.0	0.0	0.0	0.0	0.0
Receivables from related parties	0.0	-	-	0.0	0.0	0.0	0.0	0.0
Inventories	0.0	0.0	0.0	0.0	0.1	0.5	0.6	0.7
Prepaid expenses and other current assets	0.1	0.2	0.2	0.1	1.5	5.0	6.5	7.8
Total Current assets	**1.0**	**0.7**	**1.0**	**1.0**	**18.4**	**55.1**	**84.7**	**125.8**
Property, plant and equipment, net	0.1	0.1	0.0	0.0	0.3	1.3	2.5	4.0
Intangible assets, net	0.1	2.5	1.7	0.0	0.2	0.6	1.3	2.0
Investments in associated companies	-	0.1	-	-	-	-	-	-
Deposits	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.1
Total non-current assets	**0.2**	**2.8**	**1.8**	**0.1**	**0.5**	**1.9**	**3.8**	**6.0**
Total Assets	**1.2**	**3.5**	**2.8**	**1.1**	**18.9**	**57.0**	**88.5**	**131.8**
LIABILITIES AND STOCKHOLDERS DEFICIT								
Bank overdraft	0.4	-	-	-	-	-	-	-
Accounts payable	1.5	0.6	0.7	0.9	8.7	19.1	16.5	11.7
Other current liabilities	1.2	0.9	2.5	1.5	3.6	12.2	15.7	19.1
Notes payable to shareholders	2.1	0.1	0.3	0.0	-	-	-	-
Accrued expenses payable to shareholders	0.8	1.0	-	-	-	-	-	-
Deferred revenues	0.1	0.1	0.3	0.4	2.4	8.1	10.4	12.6
Short term borrowings (Revolver Facility)	-	-	-	-	-	-	-	-
Total Current liabilities	**6.0**	**2.8**	**3.8**	**2.8**	**14.7**	**39.4**	**42.5**	**43.4**
Pension liabilities	1.0	1.1	2.4	2.9	2.9	2.9	2.9	2.9
Total Non Current Liabilities	**1.0**	**1.1**	**2.4**	**2.9**	**2.9**	**2.9**	**2.9**	**2.9**
Stockholders deficit	-	-	-	-	-	-	-	-
WISeKey SA	0.5	0.6	0.6	0.8	0.8	0.8	0.8	0.8
WISeTrust SA	2.3	0.4	0.4	0.4	0.4	0.4	0.4	0.4
Additional paid-in capital	65.6	76.5	105.8	111.5	122.1	122.1	122.1	122.1
Treasury shares	(2.1)	(1.7)	(1.7)	(2.0)	(2.0)	(2.0)	(2.0)	(2.0)
Accumulated deficit	(74.7)	(77.6)	(109.2)	(115.5)	(120.1)	(106.7)	(78.4)	(35.9)
Accumulated other comprehensive income	2.5	1.4	0.6	0.1	0.1	0.1	0.1	0.1
Total combined stockholders deficit	**(5.8)**	**(0.3)**	**(3.4)**	**(4.6)**	**1.4**	**14.8**	**43.1**	**85.6**
TOTAL LIABILITIES AND STOCKHOLDERS DEFICIT	**1.2**	**3.5**	**2.8**	**1.1**	**18.9**	**57.0**	**88.5**	**131.8**

Source: Research Dynamics

Cash Flow Statement

Figures in CHF'mn	2014A	2015A	2016E	2017E	2018E	2019E	2020E	2021E
Net profit/(loss) for the year	(31.7)	(6.2)	(4.6)	13.4	28.3	42.5	58.0	68.8
Non Cash adjustments	27.2	3.6	0.3	1.0	1.2	1.5	1.8	2.1
Operating profit before working capital changes	**(0.0)**	**(0.0)**	**(0.0)**	**0.0**	**0.0**	**0.0**	**0.1**	**0.1**
Decrease (increase) in trade receivables	(0.1)	(0.1)	(1.9)	(5.5)	(2.2)	(2.1)	(2.2)	(2.3)
Decrease (increase) in inventories	0.0	0.0	(0.1)	(0.3)	(0.1)	(0.1)	(0.1)	(0.1)
Decrease (increase) in other receivables	-	-	-	-	-	-	-	-
Decrease (increase) in prepaid expenses and other assets	(0.0)	0.1	(1.3)	(3.6)	(1.4)	(1.4)	(1.5)	(1.5)
Increase (decrease) in payables and other liabilities	0.1	0.2	7.8	10.4	(2.7)	(4.7)	(4.5)	(0.0)
Increase (decrease) in other current liabilities	1.6	(1.0)	2.1	8.6	3.5	3.4	3.5	3.7
Increase (decrease) in deferred revenues	0.3	0.1	1.9	5.7	2.3	2.2	2.3	2.4
Interest paid	(0.0)	-	-	-	-	-	-	-
Interest received	0.0	-	-	-	-	-	-	-
Other items	-	(0.0)	-	-	-	-	-	-
Net cash generated from operating activities	**(2.8)**	**(3.5)**	**4.1**	**29.7**	**28.9**	**41.2**	**57.4**	**73.0**
Acquisition of WISeKey Liber, net of cash acquired	-	-	-	-	-	-	-	-
Other Acquisitions	-	-	-	-	-	-	-	-
Increase in receivables from related parties	-	(0.0)	-	-	-	-	-	-
Purchase of intangible assets	(0.1)	-	(0.1)	(0.5)	(0.6)	(0.7)	(0.9)	(1.0)
Change in receivable from shareholders	(0.0)	0.0	-	-	-	-	-	-
Purchase of property, plant and equipment	-	-	(0.6)	(1.9)	(2.5)	(3.0)	(3.5)	(4.1)
Net cash flow from/(used in) investing activities	**(0.1)**	**(0.0)**	**(0.7)**	**(2.4)**	**(3.1)**	**(3.7)**	**(4.4)**	**(5.1)**
Net cash flow from/(used in) investing activities	(0.1)	(0.0)	(0.7)	(2.4)	(3.1)	(3.7)	(4.4)	(5.1)
Increase in Share Capital	-	-	10.6	-	-	-	-	-
Increase (decrease) in bank overdrafts	-	-	-	-	-	-	-	-
Increase (decrease) in notes payable to shareholders	0.4	0.0	(0.0)	-	-	-	-	-
Increase (decrease) in short term borrowings	-	-	-	-	-	-	-	-
Proceeds from issuance of common stock	2.5	0.4	-	-	-	-	-	-
Proceeds from sales of treasury shares	0.1	3.1	-	-	-	-	-	-
Net cash (used in)/from financing activities	**3.0**	**3.5**	**10.6**	**-**	**-**	**-**	**-**	**-**
Net Increase in cash and cash equivalents	**0.0**	**(0.0)**	**14.0**	**27.3**	**25.8**	**37.5**	**52.9**	**67.9**
Cash and cash equivalents - beginning of the year	0.4	0.5	0.4	14.4	41.8	67.6	105.0	158.0
Cash and cash equivalents - end of the year	0.5	0.4	14.4	41.8	67.6	105.0	158.0	225.8

Source: Research Dynamics

Key Ratios

	2014A	2015A	2016E	2017E	2018E	2019E	2020E	2021E
Growth Ratios (YoY)								
Revenue Growth (%)	(39.8%)	(34.0%)	NM	NM	28.5%	21.5%	18.5%	16.2%
EBITDA Growth (%)	NM	NM	NM	NM	NM	48.9%	44.7%	36.9%
Net Income Growth (%)	NM	NM	NM	NM	NM	50.0%	36.6%	18.7%
Profitability Ratios (% of Revenue)								
GP Margin	61.1%	64.1%	62.1%	63.6%	67.5%	71.4%	75.1%	78.6%
EBITDA Margin	NM	NM	(15.9%)	14.5%	23.4%	28.6%	35.0%	41.2%
Operating Profit Margin	NM	NM	(16.9%)	13.5%	22.4%	27.6%	34.0%	40.2%
Net income margin	NM	NM	(16.6%)	14.0%	23.0%	28.4%	32.7%	33.4%
ROE DuPont analysis								
Net profit margin (%)	NM	NM	(16.6%)	14.0%	23.0%	28.4%	32.7%	33.4%
Turnover to asset ratio	1.1x	1.1x	2.8x	2.5x	1.7x	1.4x	1.1x	0.9x
Asset to equity ratio	(1.7x)	(0.5x)	(6.1x)	4.7x	2.5x	1.7x	1.4x	1.3x
Return on equity (%)	NM	NM	NM	NM	97.9%	66.0%	50.6%	38.7%
Total common equity	(3.4)	(4.6)	1.4	14.8	43.1	85.6	143.6	212.4
Total debt	-	-	-	-	-	-	-	-
Total Invested Capital	(3.4)	(4.6)	1.4	14.8	43.1	85.6	143.6	212.4
EBIT	(31.5)	(6.3)	(4.4)	13.9	28.8	42.8	62.0	84.9
NOPAT	(31.5)	(6.4)	(4.4)	13.9	28.8	42.8	58.2	68.7
ROIC (%)	NM	NM	NM	NM	99.5%	66.6%	50.8%	38.6%
Net Profit / Sales	NM	NM	(16.6%)	14.0%	23.0%	28.4%	32.7%	33.4%
Sales / CE	NM	NM	NM	NM	NM	NM	NM	NM
ROCE (%)	NA	NA	NA	NM	97.9%	66.0%	50.6%	38.7%
Return Ratios (%)								
Return on asset (%)	NM	NM	NM	35.3%	38.9%	38.6%	35.9%	30.1%
Return on equity (%)	NM	NM	NM	NM	97.9%	66.0%	50.6%	38.7%
Major expenses (as a % of net sales)								
COGS	38.9%	35.9%	37.9%	36.4%	32.5%	28.6%	24.9%	21.4%
Opex	NM	NM	78.0%	49.1%	44.1%	42.7%	40.1%	37.4%
Liquidity ratios (x)								
Current ratio	0.3x	0.3x	1.3x	1.4x	2.0x	2.9x	4.1x	5.0x
Quick ratio	0.3x	0.3x	1.2x	1.4x	2.0x	2.9x	4.1x	5.0x

Source: Research Dynamics

DISCLAIMER

WISeKey International Holding AG ("WIHN") is a client of Research Dynamics. The equity research report(s) are prepared for informational purposes only and are paid for by the company portrayed in the report. Research Dynamics is a division of Dynamics Group AG. Dynamics Group is an independent consultancy firm focused on strategic advisory, communication management and research and analysis.

This report (henceforth known as "document") has been drafted by the authors concerned as a non-binding opinion on the market situation and on the instruments of investment in question and compiled by Dynamics Group in order to provide background information about the companies. It is intended exclusively for the purpose of information.

Dynamics Group has not individually verified the information and data on which this document is based. All information and data in this document originate from generally available sources which the author concerned or Dynamics Group viewed as reliable at the time of drafting this document. However, no liability can be assumed for their correctness, accuracy, completeness and appropriateness – neither expressly nor tacitly. The contents of this document do not represent an assurance or guarantee by the authors concerned or Dynamics Group. Forward-looking information or statements in this document contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations

Dynamics Group shall not be liable for any consequential damage to properties – on whatever legal grounds it may be. Liability of Dynamics Group on account of premeditation or gross negligence shall remain unaffected by this.

Dynamics Group has no permission to provide assurances or assume guarantees on behalf of the companies or a third party mentioned in this document. Neither the companies mentioned in this document nor any other individual assumes liability for any loss, damage or detriment that may result from the use of this document, especially when taking decisions on investments, or from other reasons. Dynamics Group cannot be held responsible for detrimental consequences that occur or may occur due to the use or its omission based on the views and inferences contained in this document. Past performance trends of value, price or rates do not provide any indications to the future trends for an investment. Dynamics Group does not provide any guarantees for the suggested yield or the achievement of referred targets.

This document does neither represent an offer of purchase, holding or sale of any securities, money market instruments or of derivatives, nor does it contain the basis for a contract or a commitment of any kind. Every investment, for example, in debentures, shares and options, is associated with enormous risks. A decision on investment with regard to any security may not be based on this document. This document is neither an advice on investment, nor a recommendation or invitation for purchasing, holding or selling any securities, money market instruments or derivatives.

Dynamics Group does not conduct any investment business and, accordingly, does not itself hold any positions in the securities mentioned in this document. However, the respective directors, employees and contractors of Dynamics Group may hold positions in the described securities and/or options, futures and other derivatives that are based on these securities.

This document has been provided to you for information only. It may not be reproduced or distributed to others or published in any other form partially or fully.

The distribution of this document and the information contained therein may be restricted in other jurisdictions by law and persons who may come into possession of this document must be aware of possible restrictions and adhere to the same. Failure to comply with such restrictions may constitute an infringement of the laws in USA or Canada governing the securities or of the laws of any other jurisdiction.

This study is protected by the copyright laws. It may be used only for the purpose as defined in this disclaimer. Portions of the study, if quoted, must be acknowledged by indicating the source. Any use other than this shall require prior written permission by Dynamics Group. Reproduction, circulation, publication and provision of online access to the document shall be regarded as its use and the same shall require permission. Circulation of this document, especially in a foreign country, may be permitted only under the provisions of the disclaimer and the applicable regulations. Unauthorized use of the study or omission of details of the source or the acknowledgement of copyright may lead to initiation of a civil suit for damages and be liable for prosecution.

If any part or individual formulations of this disclaimer are found to be unsustainable or become unsustainable at a future date, the rest of the contents and their validity shall not be affected by it.

Dynamics Group AG

Utoquai 43
CH-8008 Zürich
Tel. +41 43 268 32 32
Fax +41 43 268 32 39

Zeughausgasse 22
CH-3011 Bern
Tel. +41 31 312 28 41
Fax +41 31 312 28 49

21, rue des Caroubiers
CH-1227 Carouge/GE
Tel. +41 22 308 62 20
Fax +41 22 308 62 36

contact@dynamicsgroup.ch

http://www.dynamicsgroup.ch