WISeKey
Press Conference
Thursday, July 14, 2016
@ 4:00pm CET
at WIDDER Hotel Zurich
“Zunft Stube”
WISeKey presents its unique Swiss cybersecurity technology for IoT
& discusses its Growth Strategy

# PART I
# SAP, Microsoft , CenturyLink and MasterCard Partnerships

WISeKey

# LATEST PARTNERSHIP ANNOUNCEMENTS

## Providing cybersecurity solutions

- CenturyLink to resell WISeKey's cybersecurity solutions – including its Managed Public Key Infrastructure (PKI) technology and services – to businesses
- WISeKey's cybersecurity solutions complement CenturyLink's Managed Security Services Suite
- Recently enhanced platform that leverages security events, advanced event management technologies and customized tools and algorithms to provide fully managed security services

## Bringing payments to luxury brand watches and wearables

- The partnership adds new devices and brands to ongoing MasterCard programs to bring payments to any consumer gadget, accessory or wearable – from fitness bands to refrigerators
- With the companies' shared commitment to advance payments security in both the physical and digital worlds, MasterCard will integrate its payments technology with WISeKey's Cryptographic Root of Trust for IoT and NFC Trusted© technology solutions
- Providing consumers with the freedom to securely shop using their favorite watch or wearable.

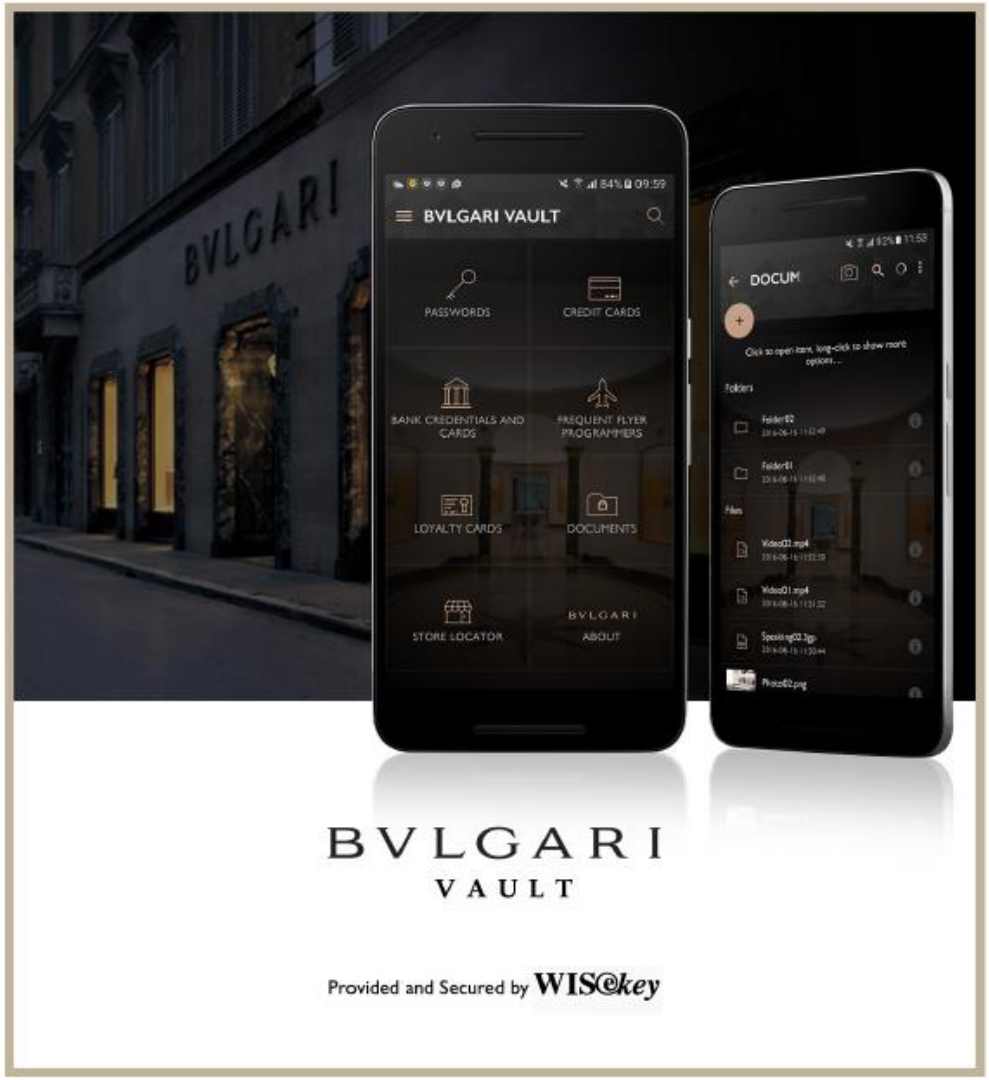
## Collaboration to Help Secure IoT Edge Devices

- The collaboration aims to allow the integration of WISeKey's Managed Cryptographic Root of Trust secure IoT Edge Device with devices leveraging SAP HANA® Cloud Platform for the Internet of Things (IoT)
- Providing increased security of IoT devices when connecting to SAP solutions for the IoT
- 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

## Bringing Innovation and Security to IoT across the Globe

- Providing smart cities with a scalable, easily manageable object identity management and security solution when connecting to Microsoft Azure and other Microsoft-based platforms
- The Managed WISeKey **Root of Trust** (RoT) serves as a common trust anchor, which is recognized by operating systems (OS) and applications to ensure the authenticity, confidentiality and integrity of on-line transactions
- With the Cryptographic RoT embedded on a device, provided by WISeKey as a hardware Secure Element or a software Certificate, the IoT product manufacturers can protect the devices and secure the interactions among and between objects and people

# BVLGARI VAULT APP TO SECURE THE FUTURE




## WISeKey adding value on the Bulgari Ecosystem

**Bulgari** is the only luxury brand to connect the world of high added value luxury products with the digital reality of today:

- The first “wrist objects”, the true main issue that technological evolution applied to watches will need to address in the future is that of the protection of digital data and its total security:
- Intuitive functioning of the application enables users to secure their data with ease
- Archive and synchronise data on a “cloud” which are then physically stored in a bunker buried in the Swiss Alps
- Encrypted technology achieves an unprecedented “asymmetrical” level customarily used by government agencies
- Password through fingerprint recognition, facial recognition as well as a four-point gesture connection to link together via the touch screen of a mobile phone
- The vault can storage credit cards, documents (including travel documents), secure message sending, scanned signature, etc.
- 1.5 million subscribers paying 45 CHF per year and vault

# PART II
# WISeKey Cybersecurity Platform Growth Strategy in EU, USA, China and India

WISeKey

# PATENTED AND ESTABLISHED TECHNOLOGY

## Strong U.S. Go-To-Market Driven By Strong Channel Partnerships and Patented Technology

Microsoft

WISeKey and Microsoft enlisted in a **partnership to deliver digital identity** management solutions to governments around the world

CityNext

WISeKey will be contributing **three solutions (WISeAuthentic, WISeKey, and WISeID)** to Microsoft's CityNext initiative to make cities smarter, more efficient, and safer

SAMSUNG

WISeKey recently reached an agreement with Samsung to install their **unique NFC authentication** and tracking technology in Samsung's smartphones

hp

WISeKey partnered with HP in 2002 to bring **e-voting to Switzerland** for the first time and has maintained a strong relationship with HP since then

- One of a limited number of companies with a Root Certificate product
- Only independent security company with a PKI root key – new applicant would take 5 years to secure
- Unique IP and IoT Patents - USA patent in IoT granted, in addition to Switzerland and Singapore

## Industry-respected Thought Leadership

- Distinctive authority and thought leader on topic of digital identity protection and cyber security
- Advisory board with experience in different industries and sectors relevant to WISeKey

CLINTON GLOBAL INITIATIVE · WORLD ECONOMIC FORUM · UNITED NATIONS · THE WORLD BANK · THE GLOBAL COMPACT

## Opportunities for Expansive Growth

- Pursue growth through existing and new clients, including multi-national companies
- Expand partnerships and existing relationships with multi-brand companies
- Expand leadership team to manage growth
- Development of a US Cyber Security Bunker
- Potential acquisitions that allow access to new vertical or add new products, services and geographies
- Expand operations in Switzerland, Asia, and Latin America

# KEY MILESTONES – PROVEN TRACK RECORD SINCE THE INCORPORATION IN 1999

**1999:** *Incorporation of WISeKey SA by Carlos Moreira*

**2003:** *First ever binding Internet vote in the Canton of Geneva using biometric enabled public key infrastructure*

**2005:** *Security products for computers and digital video broadcasting*

**2006:** *Launch of CertifyID product for digital certification and identity management*

**2007:** *Secure registration and access control of online offerings, dematerialization and secure electronic document dematerialization*

**2008:** *Citizen Services Platform in partnership with Microsoft for confirming citizen access to government services and validity of citizen electronic*

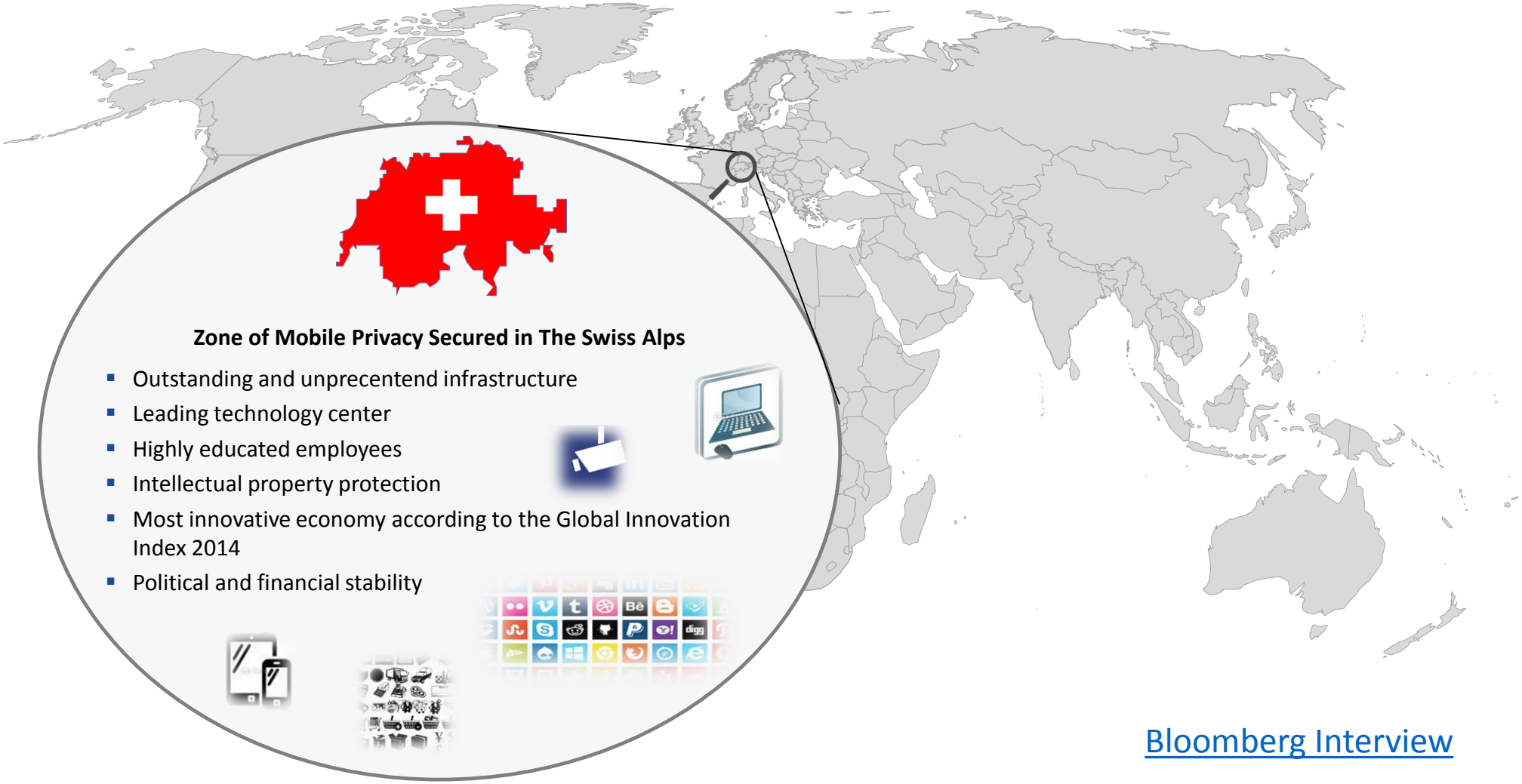
**2011:** *WISeID and WISfans mobile products for securing social media applications and for effective data protection*

**Transitional years**

**2014:** *WISeAuthentic for the security of luxury goods, artwork, pharmaceuticals, spare parts and VIP social networking*

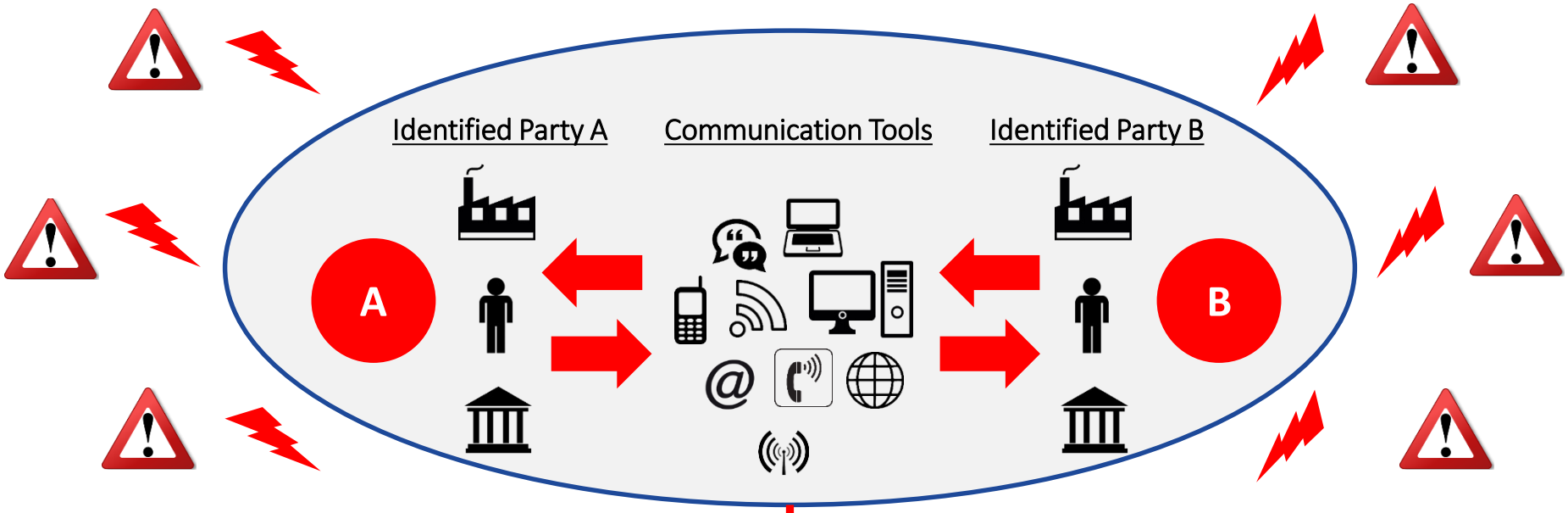
**2016:** *WISeKey International Holding listed on the SIX Swiss Exchange*

# GEOPOLITICAL ADVANTAGES




Bloomberg Interview

# WISeKey – CURRENT PRODUCT RANGE & MARKET SOLUTION




WISeKey

**WISeAuthentic**

*Anti-Counterfeiting and Sales Monitoring System - 100% Authentication*

**NFC Trusted**

*Integrates wearable technology in physical and virtual environments and empowers them to become transactional devices*

*IoT / Digital Brand Management*

*Cybersecurity Services*

**WISeSecurity**

*Comprehensive Security and Managed PKI for Governments and Corporations*

*Mobile Security*

**WISWATCH**

*NFC Watch Pairs with Mobile Phone App to provide a Trusted Key to the data*

**WISeid**

*Protection of identity and information through a secure personal cloud*
*Swiss Military Grade Encryption*

# PART III
# Cyber Security Trends Creating Opportunities Across the Enterprise

WISekey

# THE CYBER SECURITY MARKET

**$75.4bn** Worldwide spending on information security in 2015

**253bn** Estimated number of free apps by 2017

**$21.4bn** Worldwide security software revenue in 2014

**>800ml** Individuals were victims of cyber rimes where their personal data was stolen

**40%** Companies that do not scan mobile apps for vulnerabilities

**$2.5m** Average total financial losses due to security incidents in 2015

**71%** Mobile apps that store data in an unsecure manner

**>4,000** Companies have been hacked in 2014

**97%** Mobile apps unintentionally reveal info of potential benefit to malicious attackers

**1.5m** Average number of cybersecurity attacks per week

**56%** Respondents saying it is unlikely that their organization will detect a sophisticated attack

**97%** Mobile applications examined that had significant flaws in their security features

**70%** Most commonly used IoT devices that contain vulnerabilities

**66%** Mobile apps that did not protect data via encrypted communication or other means

**2x** U.S. info security budgets have grown at almost double the rate of IT budgets

**76%** People believing that cyber security will become a lasting topic

**15-20%** Of the value created by the Internet, is extracted by cybercrime

**59.1m** Enterprise security managers expecting to increase their budget in the next 90 days

# OPPORTUNITY DUE TO GROWING CYBER ATTACK SURFACE

## The Growing Cyber Attack Surface

**More users**
3.0bn in 2015
4.0bn in 2019

**More smartphone connections**
3.3bn in 2015
5.9bn in 2019

**More data**
8.8 zerabytes in 2015
44.0 zerabytes in 2019

**More IP-connected devices**
16.3bn in 2015
24.4bn in 2019

**More network traffic**
72.4 exabytes per month in IP traffic 2015
168.0 exabytes per month in IP traffic 2019

## New Device Types

**Increasing number of tablets**
248 million in 2015
269 million in 2019

**More IoT devices**
15 billion in 2015
200 billion in 2020

**Global public cloud market size**
USD 97bn in 2015
USD 159bn in 2019

**More wearable devices**
200 million in 2015
780 million in 2018

# Part IV
# Three Major IoT Monetization Strategies

WISekey

The Internet of Things has the potential to change the way we work and even our daily lives

The ability to monitor and manage objects makes possible to enable a full spectrum of new solutions—to optimize systems and processes, save time for people and businesses, and improve quality of life… But such a enormous benefit brings also security risks which can’t be ignored

Fake objects interacting in networks, injection of misleading data in industrial setups, eavesdropping of confidential information… The inclusion of security techniques in the IoT is critical to enable such benefits while controlling the risks

# THREE MAJOR NEW IoT MONETIZATION STRATEGIES

**Major providers do not have yet a clear monetization strategy for IoT – there is no clear strategy on how to make money despite the potential**

- By 2017, 90 million people will live in smart homes. By 2020, there will be 50 billion connected devices. The latest Gartner forecast predicts that by 2020 there will be USD309bn in incremental revenue opportunity for IoT suppliers, mostly in services
- With numbers such as these, it's clear IoT is not just another trend – it is the future of business

1

### WISeKey Root of Trust

- Clients: Microsoft, Samsung, Centurylink, Kaspersky, SAP and MasterCard
- WISeKey gets paid a royalty for every ID in/out of the Cloud Platform

2

### WISeKey Trusted IoT Microprocessors

- Via the acquisition of VaultIC WISeKey can now enter this IoT Chip space as the smartphone era over and the key growth driver in hardware will be the Internet of Things Trusted Chips
- WISekey generates revenue (CHF35m in 2017) selling these Trusted IoT chips with the signed partners (SAP, Microsoft, MasterCard, Samsung, Centurylink)

3

### WISeKey IoT Payment Services

- WISeKey will benefit from payment services companies are moving to the Internet of Things
- Bloomberg report projected a huge increase in the mobile-transaction market, with payments projected to reach USD90bn in 2017, up from USD12.8bn in 2012
- WISeKey gets paid per customer using the technology

# MAJOR DIFFERENTIATION

## WISeKey Root of Trust for IoT

- Established Swiss cyber security company entering the global market; solutions generate secure digital identities for people, objects & content
- Unique Trust Model with accreditations from Standard Bodies and International Agencies
- The Root of Trust (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
- At the heart of this strategy is the OISTE-WISeKey Cryptographic Root of Trust which has been actively used since 1999 by over 2.6 billion desktop, browsers, mobile devices, SSL certificates and Internet of Things' devices
- The OISTE WISeKey Cryptographic Root of Trust is ubiquitous and universal, and a pioneer in the identification of objects.

## WISeKey adding value

- Cyber security is a major issue with the deployment of IoT on which 50 billion objects will be connected to the Internet by 2020
- WISeKey managed to register in Switzerland and USA (in competition with leading IT firms) a patent protecting IoT transactions with strong identifications
- WISeKey knows already how to monetize this sector and is commercializing the technologies with brands adding IDs on objects – no competitors are doing this
- Internet of Things (IoT) is a scenario in which objects, people and digital assets are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction
- Investments to date have positioned WISeKey to monetize the Internet of Things (IoT)
- WISeKey Identity Ecosystem is unique on the market. Patented technology in USA with high encryption and customized solutions
- Leveraging existing platform to build a leading global cyber security company; establishing a US presence , scaling and pursuing organic and external growth
- With the Cryptographic Root of Trust embedded on the device, together with it's own unique identity, can secure the interactions among objects and between objects and other entities

**WISeKey is the only company globally with a non US rootkey insures customers' information privacy which is a big concern for multi-national and non-US based companies**

ATM
Thank you for your attention!
WISekey