# WIS@key

**The Trusted Vertical Cyber Security Platform**

# Cybersecurity Mobile Solutions

**WISePhone Terminal Enterprise-grade security**

WISeKey Technology

iD

WIS@Phone

Secured by **WIS@key**

Human Bios International AG
bits for a better life

## wissens-GiPFeL
Ihr Zmorge mit frischen Informationen aus der digitalen Welt, Technik + Sicherheit

**Carlos Moreno**
VP Corporate Alliances & Parterships

📍 Kreuzlingen

⏰ 28th March 2019

✉ cmoreno@wisekey.com

**WIS@key**

# DISCLAIMER

This communication expressly or implicitly contains certain forward-looking statements concerning WISeKey International Holding Ltd and its business. Such statements involve certain known and unknown risks, uncertainties and other factors, which could cause the actual results, financial condition, performance or achievements of WISeKey International Holding Ltd to be materially different from any future results, performance or achievements expressed or implied by such forward-looking statements. WISeKey International Holding Ltd is providing this communication as of this date and does not undertake to update any forward-looking statements contained herein as a result of new information, future events or otherwise.

This corporate presentation does not constitute an offer to sell, or a solicitation of an offer to buy, any securities, and it does not constitute an offering prospectus within the meaning of article 652a or article 1156 of the Swiss Code of Obligations or a listing prospectus within the meaning of the listing rules of the SIX Swiss Exchange. Investors must rely on their own evaluation of WISeKey and its securities, including the merits and risks involved. Nothing contained herein is, or shall be relied on as, a promise or representation as to the future performance of WISeKey.

# COMPANY SNAPSHOT

WISeKey is a global leader in the delivery of integrated security products for Internet of Things ("IoT") digital identity ecosystems combined with Blockchain Technology

| | |
|---|---|
| **Founded** | 1999 |
| **Employees** | 95 worldwide |
| **Headquarters** | Geneva, Switzerland |
| **Stock Exchange*** | SIX Swiss (SWX: WIHN) |

*Announced intention to list ADR in U.S.

| | |
|---|---|
| **Core Technology** | **Cybersecurity Trust Platform** deploying trust services on cryptographic chips for the security of devices, users, and the data that they produce |

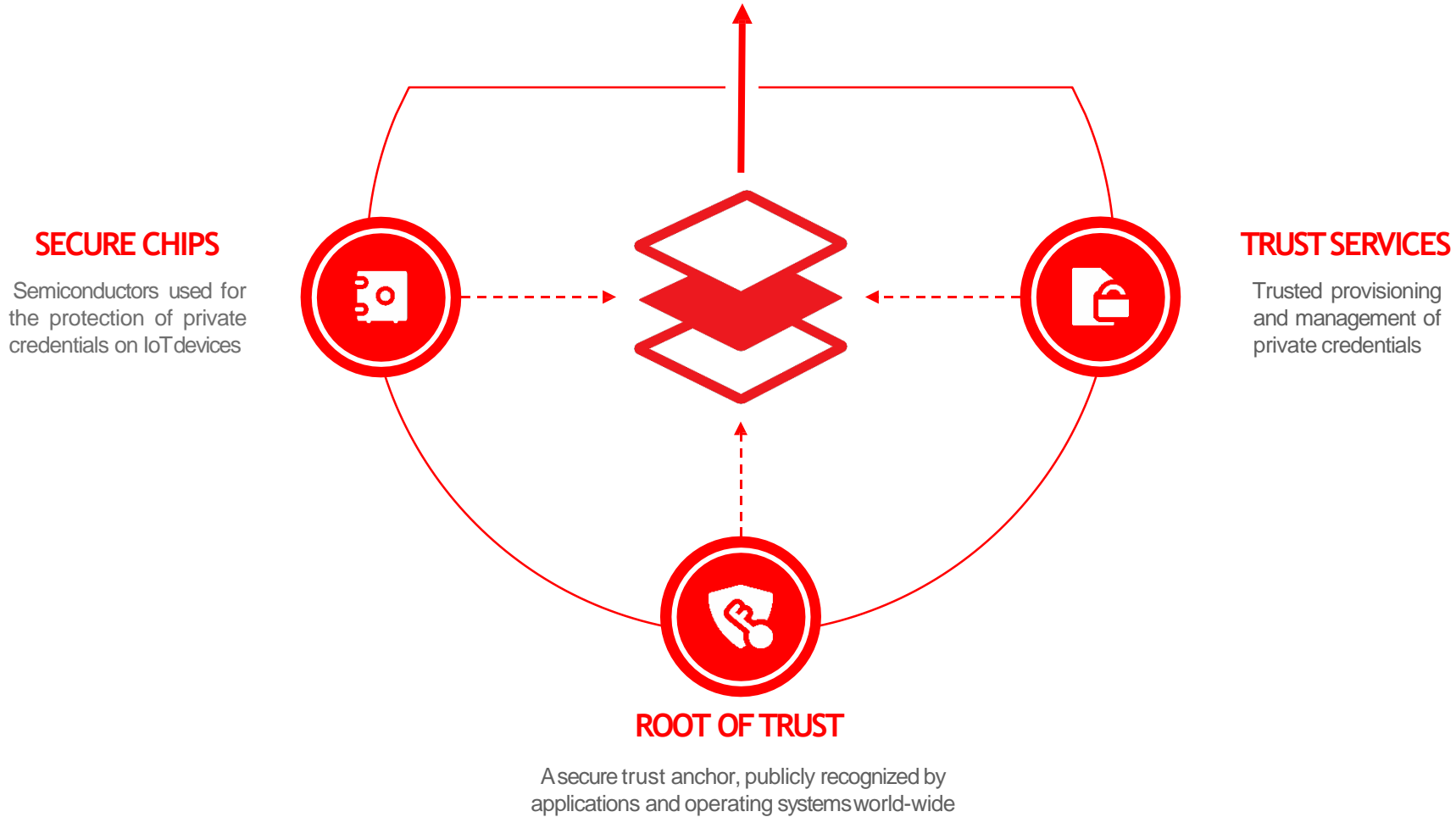| | |
|---|---|
| **Markets Served** | Secure IoT |
| | Blockchain |
| | Root of Trust |
| | Artificial Intelligence |
| | Trust Services (mPKI, eID, e-signatures) |

WIS@key

# The OISTE foundation

- 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 desktops, 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

- The OISTE Foundation was created by the WISeKey Founders to ensure the neutrality of the Trust Services

- The Foundation is regulated by the Swiss laws and enforces values to protect the Neutrality and Sovereignty of the data and identities

- WISeKey is nominated as the operator of the Trust Model, but the by-laws of the Foundation allows the participation of other players, operating their own Root of Trust

- The OISTE Foundation is recognized by the United Nation with a special ECOSOC consultative status, and participates in different initiatives promoted by UN to universalize the access to the electronic identities



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

# TECHNOLOGY LEADER

WISekey has created the world's first Cybersecurity Trust Platform
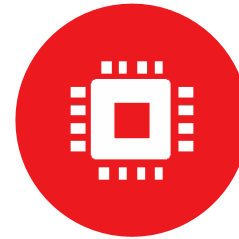that authenticates and secures devices, people, documents, and data

## SECURE CHIPS

Semiconductors used for
the protection of private
credentials on IoT devices

## TRUST SERVICES

Trusted provisioning
and management of
private credentials

## ROOT OF TRUST

A secure trust anchor, publicly recognized by
applications and operating systems world-wide

**WIS©key**

# MARKET PENETRATION

## 3.6 Billion
Browsers (total) Root of Trust installed

## 1 Billion
WISeKey VaultIC IoT chips since 2010

## 1.6 Billion
Mobile OS(total) Root of Trust installed

## 250 Million
Digitally signed emails per year

# CUSTOMER VALUE

## 3,500+ clients worldwide

WISeKey enables secure connections for **People-to-Machines** and **Machine-  to-Machines**, creating new avenues of revenue growth for our customers

| FINANCIAL SERVICES | PUBLIC SECTOR | CONSUMER / HEALTH | INDUSTRIAL / IT |
|---|---|---|---|

# WISEKEY IDENTITY LAYER - PKI ENABLED

- WISeKey Identity Layer combine's account and profile management becoming an identity provider provisioning trusted digital certificate for people, objects and servers.
- Enabling secure transactions and operations, operating strong authentication, validation, digital signature, and other access control technics.
- WISeKey enables secure connections for People-to-Machines and Machine-to-Machines, creating new avenues of revenue growth for our customers

## Object identity

- To operate a securely an IoT ecosystem, every object is verified using is the private key from the object digital certificate contain a list of attributes settled during the provisioning and is stored in an HSM.
- The attributes from the digital certificate may be associate with dynamic elements stored into the blockchain decentralized layer.
- The HSM might be embedded into a large variety of form factors.
- This identity can be suspended or revoked at any point of time don't require to have access to the HSM
- Any operation performed during the lifetime of the product will require the digital identity

## Personal identity

- Everyone to authenticate with a personal digital identity stored in an HSM (WISePhone Block, SmartCard, Cloud or other USB Token).
- This identity can be suspended or revoked at any point of time don't require to have access to the HSM.
- On each transaction verifies that the actor is legitimate, and allowed to proceed with a transaction and the transaction is digitally signed before to be into the blockchain decentralized layer.

## Servers identity

- Every server equipped with an SSL Certificate qualified enable the first level of trust
- The information send on the Internet is passed from computer to computer to get to the destination server.
- When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending such as credit card numbers, usernames and passwords, and other sensitive data's to. This protects it from hackers and identity thieves.

**WIS⊕key**

▪ **The first Swiss Designed secure blockchain smartphone with enterprise-grade security**

- Enabling Managed Services Enterprise Platform
  - The establishment of a secure ecosystem for enterprise communication
  - Encrypted end to end voice and text message communication
  - Secure data store cloud and local
  - Secure Terminal for Enterprise Access for distant collaborators and partners
  - Central and instant access revocation



**WIS⊙key**

# WISEPHONE GENESIS AND BLOCK EDITIONS

WISeOS Android based

RAM 4GB (6GB) ROM 64GB (128GB)

SoC: Mediatek Helio P23 MT6763 8 x 2GHz
eSE: VaultIC-405

**Genesis Edition** 5.99" FHD+IPS LCD / **Block Edition** 6.01" AMOLED FHD+Slim Bezel

GSM:850/900/1800/1900  WCDMA:1/8
LTE: Global Bands

Wi-Fi: a/b/g/n Bluetooth: BT 4.0 LE NFC: ST21NFCD

Main: Sony 21MP PDAF Front: OV 13MP

G/P/L, e-Compass, Gyro, Fingerprint sensors

GPS/GLONASS

5000mAh
QuickCharge (9V/2A) 10W Wireless Charging

155 x 75 x 9.5 mm

170 g

**Genesis Edition** ZINK Unibody Frame Rubberised Textured Back Cover
**Block Edition** Unibody Aluminum Frame  Rubberised Textured Back Cover

WIS@key

# WISEPHONE APPLICATIONS SUITE

WISeKey Mobile Applications are
Protected against hackers reverse
engineering by code obfuscation
technology

**WISeID**
Secure profile and
account management

**WISeTalk** Secure
Business
Communications

**WISeAccess** Secure
access control

**WISeVault**
Secure data vault

**WISeSign**
Digital signature

**WISeOS**
Security hardening

**WISeEmail** Secure
Email
communications

**WISeCloud**
Secure and encrypted
data store

**WISeStamp**
Objects Fingerprint
Stamped on Blockchain

**WISe@key**

# WISEKEY HSM INSIDE WISEPHONE BLOCK EDITION

## VaultIC405

WISEKEY SEMICONDUCTORS HSM


**VaultIC**

**Security Settings**

Sercure firmware

VaultIC405

WISeKey is hardening the Android Operating System integrating a WISeKey Secure Element

Kernel Firmware interface

- **Cryptographic Services**
  - Public Key Pair Generation
  - Digital Signature
  - Encryption / Decryption
  - Message Digest
  - Key Wrapping / Unwrapping
  - Random Number Generation
- **Cryptographic Algorithms**
  - DES / 3DES
  - AES 128/192/256 bits
  - GCM / GMAC
  - RSA® up to 4096 bits*
  - DSA up to 2048 bits
  - ECC up to 576 bits
- **Memory**
  - File System 16 Kbytes
  - Write Endurance 500 Kcycles / Data Retention 50 Years
  - 7-Slot ephemeral Key Ring
- **Certifications / Standards**
  - EAL4+ Ready
  - FIPS 140-2 Security Level 3
  - Microsoft Smart Card Minidriver compliant
  - SSL support
  - PKCS#11

Secure Element HSM

Android **Harndening**

WIS@key

# WISEPHONE APPLICATIONS SUITE

## WISeOS

WISEKEY SECURITY SETTINGS
CONFIGURE SECURITY LEVEL AND PRIVACY POLICIES

**Features**

- WISEKEY ACCOUNT
- DIGITAL IDENTITIES
- SECURE AUTHENTICATION
- INDUSTRIALIZATION

Security Settings

VaultIC405

**Settings**

- **Sound** — Volume, vibration, Do Not Disturb
- **Storage** — 33% used - 42.86 GB free
- **Security & Location** — Screen lock, fingerprint
- **Users & accounts** — Current user: Gaetan Agilulf
- **Accessibility** — Screen readers, display, interaction controls
- **WISeKey Security**
- **Google** — Services & preferences
- **System** — Languages, time, backup, updates

- **Key features**
  - Security parameters and management are placed at the System and can be used by all applications to protect data and enforce privacy in respect of the GDPR

  - WISeKey Semiconductors
    - WISeKey VaultIC HSM
    - Integration with WISeOS Edition

  - WISeKey ID Federation
    - WISeKey Authorization Services

  - WISeKey Security
    - WISeKey Accounts
    - WISeKey Digital Identiity
    - Prevent access

  - WISeKey Factory Provisioning
    - WISeIDProvising
    - Not connected to the GooglePlaystore

Secure Element HSM     Security management     Android **Harndening**

# WISEPHONE APPLICATIONS SUITE

## WISeID

PROTECT AND MANAGE YOUR IDENTITIES



- **Key features**
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - Account management
  - Multiple account support
  - Universal authentication & authorization platform for web, mobile and legacy applications
  - Digial Certificate provisioning and management (WISePhone HSM or/and Cloud HSM)
  - Optional Video KYC Service for onboarding
  - WISeKey Secure Internet Browser
  - This application is protected against hackers reverse engineering using code obfuscation technology

| KYC | Identity management | Profile management | Cloud HSM Digital Certificate | Secure Element HSM |
|-----|---------------------|--------------------|-------------------------------|--------------------|

**WIS⊕key**

# WISEPHONE APPLICATIONS SUITE

## WIS@TOlk

### PPROTECTING VOICE AND TEXT COMMUNICATIONS

### Voice
Secure calls and conferences with end-to-end encryption. Integration with PBX systems to complement the telephony services in organizations with a secure single number extension.

### Messaging
Instant messaging services with group functionality for secure communication and collaboration. Complemented by secure SMS when no data connection is available.

### Files
Send pictures, videos, voice messages and documents from the application without leaking data in the end-user device. Keep them securely in a container and control their access.
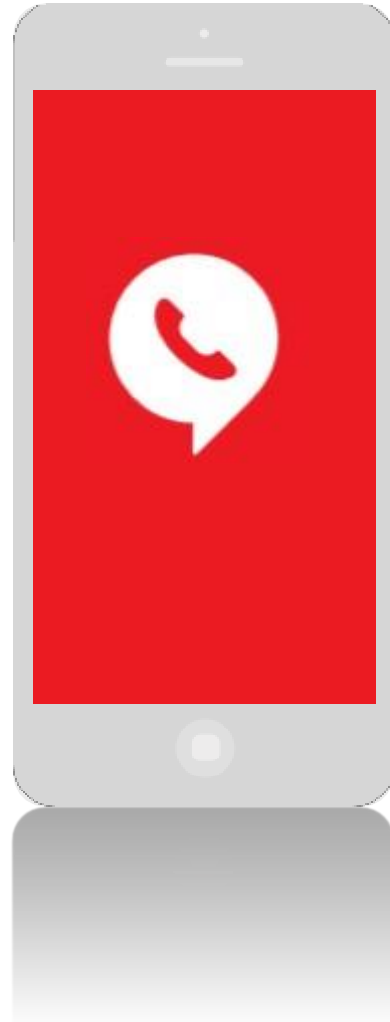
- **Key features**
  - Voice calls
  - Conference calls
  - External calls
  - Instant messaging
  - Group messaging
  - Secure SMS
  - File transfer
  - Message auto-destruction
  - Call recording
  - Centralized management
  - End-to-end encryption
  - Secure container
  - Security policies
  - Strong crypto algorithms
  - Remote wiping
  - Device authorization control
  - Document access control
  - Restricted certificate validation
  - Double encrypon layer
  - HSM integration (PKCS#11)
  - WISeID Federation Enabled

**WIS@key**

14

# WISEPHONE APPLICATIONS SUITE

## WIS@Stamp

BLOCKCHAIN-BASED CERTIFIED MOBILE APPLICATION
WISEAUTHENTIC PLATFORM

### Microscan & Fingerprint
The photo converts an object in an unique identifiable pattern. This code can be associated with a digital certificate and uniquely identify the physical object.

### Immutable Data trails, proof of process
The hash is persisted in Blockchain for legal proof, including timestamping

### Data
The photo is associated with personal data, geolocalization.

### Digitally signed Certificate "The Proof"
Paper certificate is generated with Blockchain links, QR code, timestamping, etc.

media725710042...

File information

File name
media7257100426625489192.jpeg

Upload status
hash was submitted to originstamp

Location information

Location
46.210402, 6.143205

**Key features**

- Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
- Trusted Digital Identity
- Trusted and legally binding Digital signature
- Microscanning
- Hashing
- Medias, objects authenticity
- Encryption
- Generate object identity
- Certified Atomic timestamping
- Geolocalize operation
- This application is protected against hackers reverse engineering using code obfuscation technology

For
- Anticounterfeiting
- Traçabiliy
- Proof of ownership
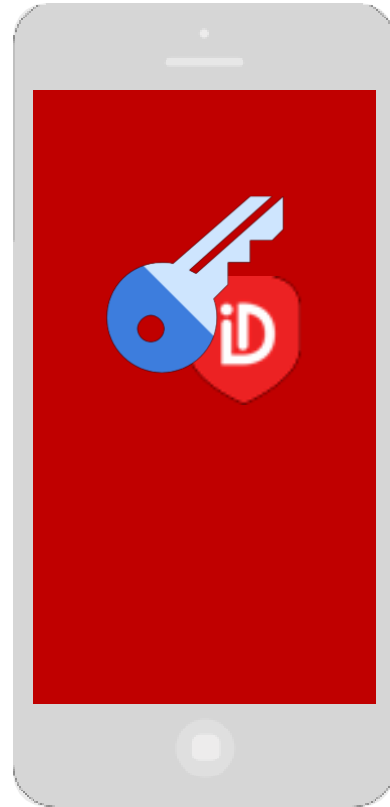- And more…

Computer Vision API      Originstamp API

WIS@key

# WISEPHONE APPLICATIONS SUITE

## WISeAccess

SECURING LOGICAL AND PHYSICAL ACCESS CONTROL

### Access management
- Create Identification methods
- Authorizations and access control
- Second factor authentication

- **Key features**
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - Multi Identification Methods (OTP, QR Codes, Pin, Generated Passwords)
  - Token service
  - This application is protected against hackers reverse engineering using code obfuscation technology
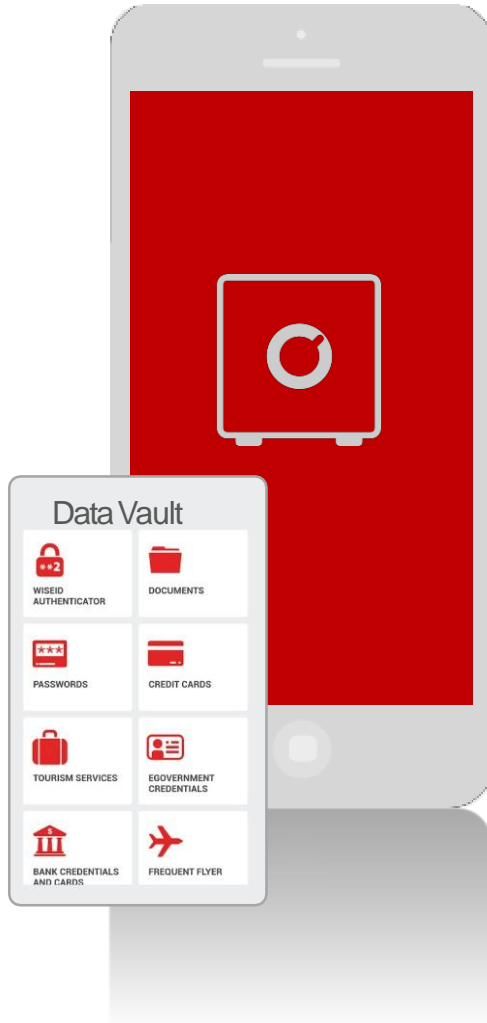
Access control

WIS@key

# WISEPHONE APPLICATIONS SUITE

## WISeVault

PROTECTING YOUR DATA & DIGITAL ASSETS

Data Vault

| | |
|---|---|
| WISEID AUTHENTICATOR | DOCUMENTS |
| PASSWORDS | CREDIT CARDS |
| TOURISM SERVICES | EGOVERNMENT CREDENTIALS |
| BANK CREDENTIALS AND CARDS | FREQUENT FLYER |

- **Key features**
  - Secure data vault for data and media encrypted storage
  - Military grade encryption AES256 bit
  - Secure password generation
  - Secure internal browser with safe one-touch enterprise portal logon
  - WISeKey Secure Internet Browser
  - WISeID Federation Enabled
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - This application is protected against hackers reverse engineering using code obfuscation technology

Encrypted Data vault

# WISEPHONE APPLICATIONS SUITE

# WISeSign

ENABLES DIGITAL SIGNATURE LEGALLY
BOUNDED

Acts as a "Wireless Token", protecting the
private key bound to the digital certificate
issued to the user.
Combined with WISeKey Cloud HSM or/and
WISePhone Block HSM

- **Key features**
  - Documents signature enabling paper less and on projects digitalisation
  - Wireless Token protecting the private key bound to the personal digital certificate issued and stored in WISeKey cloud HSM.
  - On WISePhone Block both options would be available storage in WISeKey Cloud HSM or WISePhone HSM
  - Ensures the legal validity of the digital signatures, user is always in control of the key
  - WISeKey Secure Internet Browser
  - WISeID Federation Enabled
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - This application is protected against hackers reverse engineering using code obfuscation technology
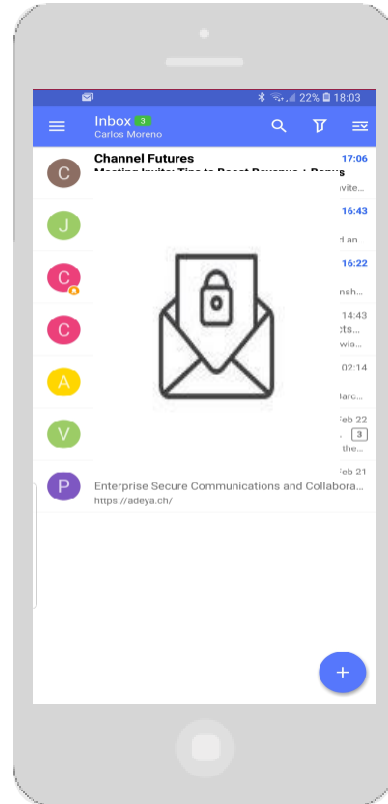
# WISEPHONE APPLICATIONS SUITE

## WISeEmail

SECURING EMAIL COMMUNICATIONS

### Securing email communication
- Email is not only the most common form of communication, but it is also the most popular vector for cyberattacks.
- From identity theft attacks like CXOsfraud, a single malicious email can cause significant brand damage and financial loss.
- The use of digital signature to assure the origine of messages is the better way to be defend against many attacks.

Inbox 3
Carlos Moreno

Channel Futures 17:06

Enterprise Secure Communications and Collabora...
https://adeya.ch/

- ▪ Key features
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - WISeID Federation Enabled
  - Use of personal Digital Certificate X509
    - Enabling Digital Signature
    - Enabling Email Encryption
  - WISeMeail Application support MS-Exchange, Office 365 and other IBM Notes Traveler, Groupwise, Kerio, Zimbra, Horde, IceWarp, MDaemon etc) supported Exchange ActiveSync.
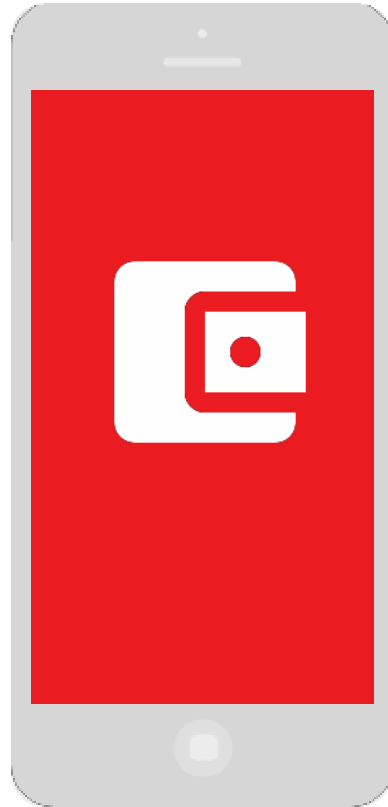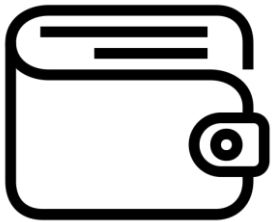  - Includes Calendar, tasks and notes

Secure Email

# WISEPHONE APPLICATIONS SUITE

## wis⊜wallet

PPROTECTING YOUR CRYPTO
TRANSACTIONS AND ASSETS

- **Key features**
  - Secure Software Wallet
  - Secure Hardware wallet embedding WISeKey Semiconductors HSM VaultIC154
  - Crypto Exchanges enabled
  - Crypto payment enabled
  - WISeID Federation Enabled
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - This application is protected against hackers reverse engineering using code obfuscation technology

Hardware
Wallet HSM

WIS⊜key

# WISEKEY SERVICES - CLOUD DATA STORAGE

## WISeCloud

PPROTECTING YOUR DATAS



- ▪ **Key features**
  - Standard communication interface
  - Encrypted Cloud data and medias storage in high-security bunkers in the Swiss Alps synced automatically
  - Support for inhouse enterprise encrypted data and medias storage synced automatically
  - Backup/restore
  - Encrypted synchronization between devices
  - Military grade encryption AES256 bit
  - WISeID Federation Enabled
  - Mobile multi authentications factors (Pin, Password, Finger Print Biometry, Face recognition, based on PKI foundation enabled by WISeKey Root of Trust
  - This application is protected against hackers reverse engineering using code obfuscation technology
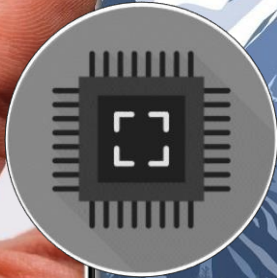
Cloud Encrypted Storage

- WISePhone Genesis commercial version Q2, April-May 2019
- WISePhone Block commercial version, Q2 June 2019

- Coming soon
  - WISePhone Enterprise Device Management and provisionning Dashboard
- …

WIS€key

**WIS@key**

The Trusted Vertical Cyber Security Platform

## Cybersecurity Mobile Solutions

WISePhone Terminal Enterprise-grade security

WISeKey Technology

# Thank You!

Kreuzlingen

28th March 2019

cmoreno@wisekey.com

**WIS@key**