

Item 1. Identity of Directors, Senior Management and Advisers

Not applicable.

Item 2. Offer Statistics and Expected Timetable

Not applicable.

Item 3. Key Information

A. RESERVED

B. Capitalization and Indebtedness

Not applicable.

C. Reasons for the Offer and Use of Proceeds

Not applicable.

D. Risk Factors

Summary of Risk Factors

Investing in our ADSs may expose you to a number of risks, including risks relating to our business and industry, financial risks, legal risks, and risks relating to our Shares and ADSs. The following summarizes part, but not all, of these risks. Please carefully consider all of the information discussed in “*Item 3. Key Information—D. Risk Factors*” and elsewhere in this annual report which contains a more thorough description of risks relating to investing in us.

Risks Relating to Our Business and Industry

- We face many risks associated with our international expansion, including geopolitical tensions, trade barriers, payment delays and currency failures.
- The future growth of the information technology and cybersecurity industry is uncertain.
- WISEKey faces intense competition from companies that are larger and better known than we are, and we may lack sufficient financial or other resources to maintain or improve our competitive position.
- If WISEKey does not successfully anticipate market needs and enhance existing products or develop new products that meet those needs on a timely basis, WISEKey may not be able to compete effectively and WISEKey's ability to generate revenues will suffer.
- Some of our larger opportunities depend on our customers’ ability to be awarded significant regional or national contracts in order to fulfil the volume predictions that were used in the pricing negotiations and forecasts.
- WISEKey's reputation and business could be harmed based on real or perceived shortcomings, defects or vulnerabilities in our security solutions or the failure of our security solutions to meet customers' expectations.
- We depend on highly skilled key personnel to operate our business, and if we are unable to attract, retain, and motivate qualified personnel, our business could be harmed.
- One of the cryptographic rootkeys used by WISEKey is owned by the *Organisation Internationale pour la Sécurité des Transactions Electroniques* OISTE. The *Organisation Internationale pour la Sécurité des Transactions Electroniques* OISTE has granted us a perpetual license to exclusively use the cryptographic rootkey. A termination of the license agreement would present a threat to WISEKey's existing business model.
- We are dependent on the timely supply of equipment and materials from various sub-contractors and if any one of these suppliers fail to meet, or delays, their committed delivery schedules due to supply chain disruptions or other reasons, we can suffer with lower or lost revenues.

- Failure of our third-party suppliers to handle increased volume for their services could impact our ability to take advantage of upside business opportunities.
- The semiconductor industry is highly cyclical.
- The demand for our semiconductor products depends to a significant degree on the demand for our customers' end products.
- We derive a significant amount of our revenues each year from a limited number of significant customers.
- The use of cryptography is subject to a variety of laws around the world. Unfavorable developments in legislation and regulation may adversely affect our business, operating results, and financial condition.
- Changes in regulations or citizen concerns regarding privacy and protection of citizen data, or any failure or appearance of failure to comply with such laws, could diminish the value of our services and cause us to lose customers and revenue.
- Cybersecurity incidents, including data security breaches or computer viruses, could harm our business by disrupting our delivery of services, damaging our reputation or exposing us to liability.

Financial Risks

- WISEKey has a history of losses and may not achieve profitability in the future.
- Certain of the Company's large shareholders, including if acting in concert, may be able to exert significant influence on the Company and their interests may conflict with the interests of its other shareholders.
- Our operating results can vary significantly due to the impairment of goodwill and other tangible and intangible assets due to changes in the business environment.
- We may need additional capital in the future and it may not be available on terms favorable to us or at all.
- The Company is a holding company with no direct cash generating operations and relies on its subsidiaries to provide it with funds necessary to pay dividends to shareholders.

Legal Risks

- We are subject to anti-takeover provisions.
- We may become exposed to costly and damaging intellectual property or liability claims, and our product liability may not cover all damages from such claims.
- We process and store personal information, which subjects us to data protection laws and contractual commitments, and our actual or perceived failure to comply with such laws and commitments could harm our business.

Risks Related to Our Shares and ADSs

- As a foreign private issuer, we are exempt from certain disclosure requirements under the Exchange Act, which may afford less protection to our shareholders and ADS holders than they would enjoy if we were a domestic U.S. company.
- We may lose our foreign private issuer status, which would then require us to comply with the Exchange Act's domestic reporting regime and cause us to incur significant legal, accounting and other expenses.
- We have never paid dividends on our share capital, and we do not anticipate paying cash dividends in the foreseeable future.
- ADS holders may not be entitled to a jury trial with respect to claims arising under the deposit agreement, which could result in less favorable outcomes to the plaintiffs in any such action.
- You may not receive distributions on our Class B Shares or any value for them if it is illegal or impractical to make them available to you as an ADS holder.
- The rights accruing to holders of our shares may differ from the rights typically accruing to shareholders of a U.S. corporation.

Risks Related to Our Business and Industry

COVID-19 and prolonged economic uncertainties or downturns have adversely affected our business and could materially adversely affect our business in the future.

Our business depends on our current and prospective customers' ability and willingness to spend money in security applications, and on our suppliers' ability to source key components and material, which are both in turn dependent upon the overall economic health.

Global negative economic conditions due to the COVID-19 pandemic caused some of our customers to delay their orders, in the year 2020 in particular, and caused a global shortage in semiconductors' material sourcing which will continue in the short-term future. Further economic uncertainties have been brought on by the current conflict between Russia and Ukraine, which may also further affect the sourcing of certain materials. Although we do not have any customer exposure in Eastern Europe, the overall economic impact of this conflict is still unknown. Many customers and prospects of WISEKey are manufacturers of electronic devices. Our business depends on their ability to produce their devices. If they encounter shortages in the supply of crucial components, they will slow down the production and thus also reduce their orders of WISEKey semiconductors to avoid idle stocks in their just in time provisioning.

As a result of the overall impact of COVID-19, political tensions, conflicts and other conditions resulting from financial and credit market fluctuations, there could be a decrease in corporate spending on information security software. Continuing economic challenges may cause our customers to re-evaluate decisions to purchase our solution or to delay their purchasing decisions, which could adversely impact our results of operations.

We are currently operating in a period of economic uncertainty and capital markets disruption, which has been significantly impacted by geopolitical instability due to the ongoing military conflict between Russia and Ukraine. Our business, financial condition and results of operations may be materially adversely affected by any negative impact on the global economy and capital markets resulting from the conflict in Ukraine or any other geopolitical tensions.

U.S. and global markets are experiencing volatility and disruption following the escalation of geopolitical tensions and the start of the military conflict between Russia and Ukraine.

In February 2022, a full-scale military invasion of Ukraine by Russian troops was reported. Although the length and impact of the ongoing military conflict is highly unpredictable, the conflict in Ukraine could lead to market disruptions, including significant volatility in commodity prices, credit and capital markets, as well as supply chain interruptions. We are continuing to monitor the situation in Ukraine and globally and assessing its potential impact on our business. Additionally, Russia's prior annexation of Crimea, recent recognition of two separatist republics in the Donetsk and Luhansk regions of Ukraine and subsequent military interventions in Ukraine have led to sanctions and other penalties being levied by the United States, European Union and other countries against Russia, Belarus, the Crimea Region of Ukraine, the so-called Donetsk People's Republic, and the so-called Luhansk People's Republic, including agreement to remove certain Russian financial institutions from the Society for Worldwide Interbank Financial Telecommunication, or SWIFT, payment system, expansive ban on imports and exports of products to and from Russia and ban on exportation of U.S. denominated bank notes to Russia or persons located there. Additional potential sanctions and penalties have also been proposed and/or threatened. Russian military actions and the resulting sanctions could adversely affect the global economy and financial markets and lead to instability and lack of liquidity in capital markets. Although our operations have not experienced material and adverse impact on supply chain, cybersecurity or other aspects of our business from the ongoing conflict between Russia and Ukraine, there is no assurance that such conflict would not develop or escalate in a way that could materially and adversely affect our business, financial condition, and results of operations in the future.

We face many risks associated with our international expansion, including geopolitical tensions, trade barriers, payment delays and currency failures.

We are continuing to expand our operations into additional international markets. The expansion into international markets may cause difficulties because of distance, as well as language and cultural differences. Other risks related to international operations include fluctuations in currency exchange rates, difficulties arising from staffing and managing foreign operations, legal and regulatory requirements of different countries, and overlapping or differing tax laws. Management cannot assure that it will be able to market and operate WISEKey's services successfully in foreign markets, select appropriate markets to enter, open new offices efficiently or manage new offices profitably.

Offering our services in a new geographical area also poses geopolitical risks. For example, export and import of cryptographic technologies is subject to sanctions, and national import and export restrictions. Changes in these restrictions due to geopolitical tensions may significantly harm our business.

As a result of these obstacles, we may find it impossible or prohibitively expensive to enter additional markets, or our entry into foreign markets could be delayed, which could hinder our ability to grow our business.

Business practices in the global markets that we serve may differ and may require us to include non-standard terms in customer contracts, such as extended payment or warranty terms. To the extent that we enter into customer contracts that include non-standard terms related to payment, warranties or performance obligations, our results of operations may be adversely impacted.

Additionally, our global sales and operations are subject to a number of risks, including the following:

- difficulty in enforcing contracts and managing collections, as well as long collection periods;
- costs of doing business globally, including costs incurred in maintaining office space, securing adequate staffing and localizing our contracts;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risk of unexpected changes in regulatory practices, tariffs, tax laws and treaties;
- compliance with anti-bribery laws;
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results, and give rise to restatements of, or irregularities in, financial statements;
- social, economic and political instability, terrorist attacks and security concerns in general;
- reduced or uncertain protection of intellectual property rights in some countries; and
- potentially adverse tax consequences.

These factors could harm our ability to generate future global revenues and, consequently, materially impact our business, results of operations and financial condition.

Global inflationary pressure may have an adverse impact on our gross margins and our business.

As of the date of this annual report, global inflationary pressure has not materially affected our gross margins and our business. Our suppliers, which are all based in Asia, have not been impacted by the price inflation for energy that Europe and other geographies have experienced, nor from some raw material price inflation which might impact other industries. For fiscal year 2023, we do expect to incur significant payroll cost increases for some of our employees in order to retain and hire engineers given the strong local demand for experienced software and hardware engineers. While we believe that these costs will be balanced by the US Dollar to Euro exchange rate evolution which has absorbed the extra costs caused by the salary increase, there is no assurance that this cost balance will continue. Accordingly, continued inflationary pressure may have an adverse impact on our gross margins and could have a material adverse effect on our business, financial condition, results of operations or cash flows.

The future growth of the information technology and cybersecurity industry is uncertain.

Information (including cybersecurity) technology companies are generally subject to the following risks: rapidly changing technologies; short product life cycles; fierce competition; aggressive pricing and narrow profit margins; the loss of patent, copyright and trademark protections; cyclical market patterns; evolving industry standards; and frequent new product introductions. Technology companies may be smaller and less experienced companies, with limited product lines, markets or financial resources and fewer experienced management or marketing personnel. Information technology company stocks, especially those which are Internet related, have experienced extreme price and volume fluctuations that are often unrelated to their operating performance.

We depend on our ability to keep pace with technical advances in cryptography and semiconductor design.

WISeKey needs to keep pace with changing technologies in order to provide effective identification and authentication solutions. In addition, we need to continue adjacent and inorganic growth in order to broaden and strengthen the portfolio of products and stay ahead of the technology changes and risks in order to be successful.

WISeKey needs to anticipate, and quickly react to, rapid changes occurring in security and communications technologies and to the development of new and improved devices, services, semiconductors and software that result from these changes. WISeKey must also continue to move vertically up the value chain with its customers in order to secure future business and substantiate growth. If WISeKey is unable to respond quickly and cost-effectively to changing communications technologies, hardware and software technologies and evolving industry standards, the existing offering could become non-competitive and WISeKey may lose market share. WISeKey's success will depend, in part, on its ability to effectively use leading technologies critical to the business, enhance its existing solutions, find appropriate technology partners, and continue to develop new solutions and technology that address the increasingly sophisticated and varied needs of its current and prospective clients and their customers and its ability to influence and respond to technological advances, emerging industry and regulatory standards and practices and competitive service offerings. WISeKey's ability to remain technologically competitive may require substantial expenditures and lead-time and the integration of newly acquired technologies will also take time. If WISeKey is unable to adapt and integrate in a timely manner to changing market conditions or customer requirements, its business, financial condition and results of operations could be seriously harmed.

WISeKey faces intense competition from companies that are larger and better known than we are, and we may lack sufficient financial or other resources to maintain or improve our competitive position.

The digital security market space in which we operate face intense competition, constant innovation and evolving security threats. There are several global security companies with strong presence in this market, including VeriSign, Inc., DigiCert Inc., Entrust Datacard, Let's Encrypt, Symantec Corporation, FireEye, Inc., Red Hat Software, VASCO Data Security International, Inc., Zix Corp, NXP Semiconductors, Infineon Technologies, STMicroelectronics and Samsung Electronics. As we integrate and move into the knowledge automation space there are also related data lake and automation companies with strong foundations including Palantir and Snowflake.

Some of our competitors are large companies that have the technical and financial resources and broad customer bases needed to bring competitive solutions to the market and already have existing relationships as a trusted vendor for other products. Such companies may use these advantages to offer products and services that are perceived to be as effective as ours 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 our current security solutions and respond more quickly and effectively than we do to new or changing opportunities, technologies, standards or client requirements. Additionally, we may compete with smaller regional vendors that offer products with a more limited range of capabilities that purport to perform functions similar to our security solutions. Such companies may enjoy stronger sales and service capabilities in their particular regions.

WISeKey's competitors may have competitive advantages, such as:

- greater name recognition, a longer operating history and a larger customer base;
- larger sales and marketing budgets and resources;
- broader distribution and established relationships with distribution partners and customers;
- greater customer care and support resources;
- broader supply chains;
- greater resources to make acquisitions;
- larger intellectual property portfolios; and
- greater financial, technical and other resources.

Our current and potential competitors may also establish cooperative relationships among themselves or with third parties that may further enhance their resources. Current or potential competitors may be acquired by third parties with access to greater available resources. As a result of such acquisitions, our current or potential competitors may be able to adapt more quickly to new technologies and customer needs, devote greater resources to the promotion or sale of their products and services, initiate or withstand substantial price competition, take advantage of other opportunities more readily or develop and expand their product and service offerings more quickly than we do. Larger competitors with more diverse product offerings may reduce the price of products that compete with ours in order to promote the sale of other products or may bundle them with other products, which would lead to increased pricing pressure on our products and could cause the average sales prices for our products to decline.

If WISeKey does not successfully anticipate market needs and enhance existing products or develop new products that meet those needs on a timely basis, WISeKey may not be able to compete effectively and WISeKey's ability to generate revenues will suffer.

Many of our customers operate in markets characterized by rapidly changing technologies and business plans, which require them to adapt to increasingly complex digital security infrastructures to protect internal and external corporate communications. As our customers' technologies and business plans grow more complex, we expect them to face new and increasingly sophisticated threats of security breach or counterfeiting. WISeKey faces significant challenges in ensuring that our security solutions effectively protect identities of individual customers, company information and their brands in addition to driving efficient operations through automated decision making. As a result, we must continually modify and improve our products in response to changes in our customers' technology infrastructures.

WISeKey may not be able to successfully anticipate or adapt to changing technology or customer requirements on a timely basis or at all. If we fail to keep up with technological changes or to convince our customers and potential customers of the value of our security and automation solutions even in light of new technologies and integration, our business, results of operations and financial condition could be materially and adversely affected.

WISeKey cannot guarantee that it will be able to anticipate future market needs and opportunities or be able to develop product enhancements or new products to meet such needs or opportunities in a timely manner, if at all. Even if we are able to anticipate, develop and commercially introduce enhancements and new products, there can be no assurance that enhancements or new products will achieve widespread market acceptance.

Our product enhancements or new products could fail to attain sufficient market acceptance for many reasons, including:

- delays in releasing product enhancements or new products;

- failure to accurately predict market demand and to supply products that meet this demand in a timely fashion;
- failure to accurately price products and solutions;
- inability to interoperate effectively with the existing or newly introduced technologies, systems or applications of our existing and prospective customers;
- defects in our products;
- inability to integrate security and automation;
- negative publicity about the performance or effectiveness of our products;
- introduction or anticipated introduction of competing products by our competitors; and
- installation, configuration or usage errors by our customers.

If WISEKey fails to anticipate market requirements or fails to develop and introduce product enhancements or new products to meet those needs in a timely manner, that could cause us to lose existing customers and prevent us from gaining new customers, which would significantly harm our business, financial condition and results of operations.

Sometimes it will be necessary to make a product or product line obsolete and there may be negative impacts to sales or disruption to the customer base during the ramp down of that product.

All products have a natural lifecycle that includes the inevitable end-of-life (“EOL”) process. During the ramping down of a product, or product family, there are many ways that our business operations can be challenged. Last time buys are a typical way for customers to deal with the EOL of a product that is still critical to one of their end products. These kinds of orders show an increase in short term sales but result in the abrupt drop off of revenue from that customer, for that product, after the last time buy is delivered. Discontinuing a product also comes with the risk that we may lose that customer for good if we do not have a replacement for the product or if they decide to look at alternative suppliers because of the change in supply.

WISEKey is subject to a number of risks associated with global sales and operations.

Business practices in the global markets that we serve may differ and may require us to include non-standard terms in customer contracts, such as extended payment or warranty terms. To the extent that we enter into customer contracts that include non-standard terms related to payment, warranties or performance obligations, our results of operations may be adversely impacted.

Additionally, our global sales and operations are subject to a number of risks, including the following:

- difficulty in enforcing contracts and managing collections, as well as long collection periods;
- costs of doing business globally, including costs incurred in maintaining office space, securing adequate staffing and localizing our contracts;
- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements;
- risk of unexpected changes in regulatory practices, tariffs, tax laws and treaties;
- compliance with anti-bribery laws;

- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
- social, economic and political instability, terrorist attacks and security concerns in general;
- reduced or uncertain protection of intellectual property rights in some countries; and
- potentially adverse tax consequences.

These factors could harm our ability to generate future global revenues and, consequently, materially impact our business, results of operations and financial condition.

Some of our larger opportunities depend on our customers' ability to be awarded significant regional or national contracts in order to fulfil the volume predictions that were used in the pricing negotiations and forecasts.

The design of many industrial device comes with the risk that the product may not see the demand that was expected in that market, or the high-volume contracts may be awarded to competing suppliers. Our customers may be bidding against several other suppliers to win a government contract and if they lose the bid, we will not see the results that were originally expected during the forecasting of the opportunity size and profitability.

The shift into knowledge automation and artificial intelligence is unknown and unproven on a global scale.

The automation market has been moving forward with Robotic Process Automation ("RPA") for years and the demand in the market for the next evolution of such technology remains unknown. Our potential customers need to be accepting to move forward from their current business process automation and RPA implementations in order for WISEKey to be successful. The ability for WISEKey to predict the market and conditions is yet to be proven and the customer reaction remains unknown. In addition, the complex implementation in this sphere requires focused delivery resources and clear plans with the customer. Customer input and knowledge is critical to the success of knowledge automation and therefore some of WISEKey's potential success will be reliant on its customers belief in the value proposition but their ability to support the implementation.

Our research and development efforts may not produce successful products or enhancements to our security solutions that result in significant revenue or other benefits in the near future, if at all.

Investing in research and development personnel, developing new products and enhancing existing products is expensive and time consuming, and there is no assurance that such activities will result in significant new marketable products or enhancements to our products, design improvements, cost savings, revenues or other expected benefits. If we spend significant time and effort on research and development and are unable to generate an adequate return on our investment, our business and results of operations may be adversely affected. This is expected to be exacerbated in the coming year with the required integration of newly acquired knowledge automation assets which is expected to result in a more complex research and development program.

If WISEKey is unable to attract new customers, our future revenues and operating results will be harmed.

Our success depends in large part on our ability to attract new customers. The number of customers that WISEKey adds in a given period impacts both our short-term and long-term revenues. If WISEKey is unable to successfully attract a sufficient number of new customers, we may be unable to generate revenue growth.

A large amount of investment in sales and marketing and support personnel is required to attract new customers. If we are unable to convince these potential new customers of a need for our products or if we are unable to persuade them of our products' efficacy, we may be unable to achieve growth and there may be a meaningful negative impact on future revenues and operating results.

If we experience software errors and non-compliance, this may affect our reputation and our financial results.

WISeKey's software applications are complex, the addition of newly acquired assets increases this complexity and there is a risk that defects or errors could arise, particularly where new versions or enhancements are released. Similarly, regulatory and industry requirements are continuously evolving and we may not be able to keep up with them. This could result in adverse consequences for us, such as lost revenue, a delay in market acceptance or customer claims.

If we experience security breaches, we could be exposed to liability and our reputation and business could suffer.

We operate sensitive public key infrastructure ("PKI") platforms, retain certain confidential customer information in our secure data centers and registration systems, and our digital certificates and electronic signatures may be used by customers in mission critical applications. It is critical to our business strategy that our facilities and infrastructure remain secure and are perceived by the marketplace to be secure. We may have to expend significant time and money to maintain or increase the security of our facilities and infrastructure. Despite our security measures, our infrastructure may be vulnerable to physical break-ins, computer viruses, attacks by hackers or similar disruptive problems. It is possible that we may have to expend additional financial and other resources to address such problems. In the event of a security breach, we could face significant liability, customers could be reluctant to use our services and we could be at risk for loss of various compliance certifications needed for the operation of our businesses.

WISeKey's reputation and business could be harmed based on real or perceived shortcomings, defects or vulnerabilities in our security solutions or the failure of our security solutions to meet customers' expectations.

Organizations are facing increasingly sophisticated digital security threats and threats of counterfeiting. If WISeKey fails to identify and respond to new and increasingly complex methods of counterfeiting products or hacking personal and corporate digital accounts, our business and reputation will suffer. In particular, WISeKey may suffer significant adverse publicity and reputational harm if any of our products fail to perform as advertised. An actual or perceived breach of our customers' sensitive business data, regardless of whether the breach is attributable to the failure of our products, could adversely affect the market's perception of the efficacy of our security solutions and current or potential customers may look to our competitors for alternatives to our security solutions. Similarly, an actual or perceived failure of our product to prevent counterfeit products from being detected, regardless of whether such failure is attributable to our products, could adversely affect the market's perception of the efficacy of our authentication solutions and could encourage current or potential customers to look to our competitors for an alternative to our products. The failure of our products may also subject us to product liability lawsuits and financial losses stemming from indemnification of our partners and other third parties, as well as the expenditure of significant financial resources to analyze, correct or eliminate any vulnerability. It could also cause us to suffer reputational harm, lose existing customers or deter them from purchasing additional products and services and prevent new customers from purchasing our security solutions.

International Expansion

WISeKey's strategy includes the international expansion of its business. The expansion into international markets may cause difficulties because of distance, as well as language and cultural differences. Other risks related to international operations include fluctuations in currency exchange rates, difficulties arising from staffing and managing foreign operations, legal and regulatory requirements of different countries, potential political and economic instability, and overlapping or differing tax laws. Management cannot assure that it will be able to market and operate WISeKey's services successfully in foreign markets, select appropriate markets to enter, open new offices efficiently or manage new offices profitably. If WISeKey is not successful in accessing new markets, its results of operations and financial condition could be materially and adversely affected.

We depend on highly skilled key personnel to operate our business, and if we are unable to attract, retain, and motivate qualified personnel, our business could be harmed.

We believe that our future success is highly dependent on the talents and contributions of our senior management, including Carlos Moreira, founder and Chief Executive Officer of WISeKey, members of our executive team, and other key employees, such as key engineering, finance, research and development, marketing, and sales personnel. Our future success depends on our continuing ability to attract, develop, motivate, and retain highly qualified and skilled employees. All of our employees, including our senior management, are free to terminate their employment relationship with us at any time, and their knowledge of our business and industry may be difficult to replace.

Furthermore, our performance depends on favorable labor relations with our employees and compliance with labor laws in the countries where we have employees and plans to hire new employees. Any deterioration of current relations or increase in labor costs due to our compliance with labor laws could adversely affect our business.

Qualified individuals are in high demand, particularly in the digital industry, and we may incur significant costs to attract them. If we are unable to attract and retain our senior management and key employees, we may not be able to achieve our strategic objectives, and our business could be harmed. In addition, we believe that our senior management have developed highly successful and effective working relationships. We cannot ensure that we will be able to retain the services of any members of our senior management or other key employees. If one or more of these individuals leave, we may not be able to fully integrate new senior management or replicate the current dynamic and working relationships that have developed among our senior management and other key personnel, and our operations could suffer.

The tight global labor market has created an incredibly intense hiring environment. Since we require a highly skilled workforce in order to successfully compete in an increasingly competitive cybersecurity market, we have experienced and may continue to experience difficulty in hiring, high employee turnover, and considerable costs and productivity as well as time to market losses. In addition, to the extent we hire personnel from competitors, we may be subject to allegations that they have been improperly solicited or have divulged proprietary or other confidential information. Further, the training and integration of new employees requires allocation of a significant amount of internal resources and, even if we make this investment, there is no guarantee that existing or new personnel will remain or become productive members of our team. Our inability to attract or retain qualified personnel, or delays in hiring required personnel, particularly in sales & marketing and research & development, may seriously harm our business, financial condition and results of operations.

Furthermore, WISEKey's performance depends on favorable labor relations with our employees and compliance with labor laws in the countries where we have employees and plans to hire new employees. Any deterioration of current relations or increase in labor costs due to our compliance with labor laws could adversely affect our business.

Dependence on key personnel and loss of such key personnel may have a negative impact on the operations and profitability of WISEKey.

Our future success depends in part on the continued service of our key personnel, particularly, the members of our senior management. We have employment agreements with our key personnel, but these do not prevent such personnel from choosing to leave the Company.

One of the cryptographic rootkeys used by WISEKey is owned by the Organisation Internationale pour la Sécurité des Transactions Electroniques OISTE. The Organisation Internationale pour la Sécurité des Transactions Electroniques OISTE has granted us a perpetual license to exclusively use the cryptographic rootkey. A termination of the license agreement would present a threat to WISEKey's existing business model.

The cryptographic rootkey used by WISEKey is owned by the Organisation Internationale pour la Sécurité des Transactions Electroniques OISTE ("OISTE") acting as a trusted third party and not-for-profit entity in charge of ensuring that the Root of Trust (the "RoT") remains neutral and trusted. The name of the RoT is OISTE/WISEKey, as shown in all major current browsers that embed the rootkey. Three members of the three-member foundation board of OISTE are WISEKey board members. Members of the foundation board of OISTE are appointed by a policy authorizing authority (the "Policy Authorizing Authority" or "PAA"), whose members are international organizations, governments and large corporations that use the OISTE/WISEKey RoT. OISTE has granted us 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. A termination of the license agreement would present a threat to WISEKey's current trust model.

Services offered by our PKI business rely on the continued integrity of public key cryptography technology and algorithms that may be compromised or proven obsolete over time.

Our services and products are relying heavily on cryptography, in particular, services offered by our PKI business are based on public key cryptography technology. With public key cryptography technology, a user possesses a public key and a private key, both of which are required to perform encryption and decryption operations. The security afforded by this technology depends on the integrity of a user's private key and ensuring that it is not lost, stolen or otherwise compromised. Advances in attacks on cryptographic algorithms and technology may weaken their effectiveness, and significant new technology requirements may be imposed by root distribution programs that require us to make significant modifications to our systems or to reissue digital certificates to some or all of our customers, which could damage our reputation or otherwise harm our business. Severe attacks on public key cryptography could render PKI services in general obsolete or unmarketable.

Quantum computing may threaten the resilience of current cryptography against attacks during the current lifespan of hardware. This is certainly the case for our secure modules embedded in larger systems and/or deployed on remote locations, such as for smart meter and satellite deployments.

WISeKey cannot guarantee that its services and products will still offer sufficient protection against attacks executed with quantum computers.

We are dependent on the timely supply of equipment and materials from various sub-contractors and if any one of these suppliers fail to meet, or delays, their committed delivery schedules due to supply chain disruptions or other reasons, we can suffer with lower or lost revenues.

We use various suppliers for silicon manufacturing and testing our parts. Any one of these suppliers could not meet their commitments for on-time delivery of our products. The market supply of such products has seen and continues to see difficulties in meeting demand and these kinds of supply disruptions can happen due to global shortages of silicon wafers or chemicals used in the processing of the silicon packaging, or shortages in the labor force due to unrest or sicknesses. During the latter half of 2021 and 2022, we had to manage our delivery schedule carefully as a result of the global shortage of semiconductors material. During this period, the Company was receiving greater volumes of orders than it was capable of delivering due to such shortages, so we had to program the orders based upon the allocations of materials and production capacity available to us. While we were able to grow our revenue during this time through careful negotiation with our suppliers, we believe that our revenues would have been higher had there not been such supply disruption. Further, our business and operating conditions can be at risk if we cannot deliver on our product demand as committed in our customer contracts.

Failure of our third-party suppliers to handle increased volume for their services could impact our ability to take advantage of upside business opportunities.

We outsource several critical functions in our supply chain to third-party suppliers such as the manufacture of our semiconductors. They all have a number of risks that are present in their businesses that could limit their ability to meet increased demands if we see increased orders from our customers. If our suppliers cannot satisfy our demand, we may not be able to meet our customer demands. Also, if our suppliers add higher costs to cover their increased volume, we may see drops in our gross profit margins. Many of these costs are not fixed, even though there may be contracts in place, and may be at the discretion of the third-party vendor.

If WISeKey does not include post-quantum crypto libraries in its semiconductors, WISeKey may fail to offer its customers sufficient protection against attacks executed with quantum computers.

Quantum computing may threaten the resilience of current cryptography against attacks during the current lifespan of hardware. Certainly, in case our secure modules are embedded in larger systems and/or deployed on remote locations. This is certainly the case for smart meter and satellite deployments. WISeKey cannot guarantee that its secure modules will still offer sufficient protection against attacks executed with quantum computers. To mitigate this risk, WISeKey has launched an R&D program for assessing the portability and resistance of 2 of the algorithms shortlisted by the National Institute of Standards & Technology (NIST) as part of its Post Quantum algorithms selection contest. This program is carried in partnership with l'Ecole des Mines (one of the most prestigious French Engineering University)

If WISEKey does not respond to the trend of embedding secure modules on central processing units, WISEKey may lose the market of separate secure module chips.

The processor industry is rapidly changing with ARM-based processors that extend central processing units with ancillary functions such as graphics processing, neural processing and secure modules. WISEKey cannot guarantee that its secure modules will still be needed as separate tamper-proof chip. To mitigate this risk, WISEKey has launched an R&D program for building a “secure enclave”, which will complement its secure modules offer.

The semiconductor industry is highly cyclical.

Historically, the relationship between supply and demand in the semiconductor industry has caused a high degree of cyclicity in the semiconductor market. Semiconductor supply is partly driven by manufacturing capacity, which in the past has demonstrated alternating periods of substantial capacity additions and periods in which no or limited capacity was added. As a general matter, semiconductor companies are more likely to add capacity in periods when current or expected future demand is strong and margins are, or are expected to be, high. Investments in new capacity can result in overcapacity, which can lead to a reduction in prices and margins. In response, companies typically limit further capacity additions, eventually causing the market to be relatively undersupplied. In addition, demand for semiconductors varies, which can exacerbate the effect of supply fluctuations. As a result of this cyclicity, the semiconductor industry has, in the past, experienced significant downturns, such as in 1997/1998, 2001/2002 and in 2008/2009, often in connection with, or in anticipation of, maturing life cycles of semiconductor companies’ products and declines in general economic conditions. These downturns have been characterized by diminishing demand for end-user products, high inventory levels, under-utilization of manufacturing capacity and accelerated erosion of average selling prices. The foregoing risks have historically had, and may continue to have, a material adverse effect on our business, financial condition and results of operations.

Significantly increased volatility and instability, and unfavorable economic conditions may adversely affect our semiconductor business.

It is difficult for us, our semiconductor customers and suppliers to forecast demand trends. We may be unable to accurately predict the extent or duration of cycles or their effect on our financial condition or result of operations, and can give no assurance as to the timing, extent or duration of the current or future semiconductor business cycles generally, or specific to the markets in which we participate. In the event of a future decline in global economic conditions, our business, financial condition and results of operations could be materially adversely affected, and the resulting economic decline might disproportionately affect the markets in which we participate, further exacerbating a decline in our results of operations. The COVID-19 global pandemic, for example, created a period of significant instability in the global economy, including amongst our semiconductor clients and suppliers. The restrictions imposed upon people and businesses around the world served, in the short run, to reduce demand for our semiconductor products as many companies reduced or paused their operations. While this has since served to benefit WISEKey through the increased demand for IT network infrastructure amongst other examples, this may not always be the situation.

The semiconductor industry is highly competitive. If we fail to introduce new technologies and products in a timely manner, this could adversely affect our business.

The semiconductor industry is highly competitive and characterized by constant and rapid technological change, short product lifecycles, significant price erosion and evolving standards. Accordingly, the success of our IoT segment business depends to a significant extent on our ability to develop new technologies and products that are ultimately successful in the market. The costs related to the research and development necessary to develop new technologies and products are significant and any reduction of our research and development budget could harm our competitiveness. Meeting evolving industry requirements and introducing new products to the market in a timely manner and at prices that are acceptable to our customers are significant factors in determining our competitiveness and success. Commitments to develop new products must be made well in advance of any resulting sales, and technologies and standards may change during development, potentially rendering our products outdated or noncompetitive before their introduction. If we are unable to successfully develop new products, our revenue may decline substantially. Moreover, some of our competitors are well-established entities, are larger than us and have greater resources than we do. If these competitors increase the resources they devote to developing and marketing their products, we may not be able to compete effectively. Any consolidation among our competitors could enhance their product offerings and financial resources, further strengthening their competitive position. In addition, some of our competitors operate in narrow business areas relative to us, allowing them to concentrate their research and development efforts directly on products and services for those areas, which may give them a competitive advantage. As a result of these competitive pressures, we may face declining sales volumes or lower prevailing prices for our products, and we may not be able to reduce our total costs in line with this declining revenue. If any of these risks materialize, they could have a material adverse effect on our business, financial condition and results of operations.

The demand for our semiconductor products depends to a significant degree on the demand for our customers' end products.

The vast majority of our IoT segment revenue is derived from sales to manufacturers in the IT infrastructure (Network Servers, Switch, Home boxes, PC Keyboards, etc.), utilities distribution edge infrastructure (Smart Meters) and Access Control modules. Demand in these markets fluctuates significantly, driven by consumer spending, consumer preferences, the development of new technologies and prevailing economic conditions. In addition, the specific products in which our semiconductors are incorporated may not be successful or may experience price erosion or other competitive factors that affect the price manufacturers are willing to pay us. Such customers have in the past, and may in the future, vary order levels significantly from period to period, request postponements to scheduled delivery dates, modify their orders or reduce lead times. This is particularly common during periods of low demand. This can make managing our semiconductor business difficult, as it limits the predictability of future revenue. It can also affect the accuracy of our financial forecasts. Furthermore, developing industry trends, including customers' use of outsourcing and new and revised supply chain models, may affect our revenue, costs and working capital requirements.

If semiconductor customers do not purchase products made specifically for them, we may not be able to resell such products to other customers or may not be able to require the customers who have ordered these products to pay a cancellation fee. The foregoing risks could have a material adverse effect on our business, financial condition and results of operations.

The semiconductor industry is characterized by continued price erosion, especially after a product has been on the market.

One of the results of the rapid innovation in the semiconductor industry is that pricing pressure, especially on products containing older technology, can be intense. Product life cycles are relatively short and, as a result, products tend to be replaced by more technologically advanced substitutes on a regular basis.

In turn, demand for older technology falls, causing the price at which such products can be sold to drop, in some cases precipitously. In order to continue profitably supplying these products, we must reduce our production costs in line with the lower revenue we can expect to generate per unit. Usually, this must be accomplished through improvements in process technology and production efficiencies. If we cannot advance our process technologies or improve our production efficiencies to a degree sufficient to maintain required margins, we will no longer be able to make a profit from the sale of these products. Moreover, we may not be able to cease production of such products, either due to contractual obligations or for customer relationship reasons, and as a result may be required to bear a loss on such products. We cannot guarantee that competition in our core product markets will not lead to price erosion, lower revenue or lower margins in the future. Should reductions in our manufacturing costs fail to keep pace with reductions in market prices for the products we sell, this could have a material adverse effect on our business, financial condition and results of operations.

Our ability to forecast our future results of operations and plan for and model future growth is limited and subject to a number of uncertainties due to recent changes in our context as well as in our own sales organization and go-to-market strategies.

Even though our heritage started before 2000, much of our business has changed in recent periods. Macro changes impacting our market, particularly the digital transformation induced by the Covid pandemic, competitors suffering supply chain shortages, and the increased use of Internet of Things (IoT) resulted in growing demand for our products.

To address this demand, we made substantial investments in our sales force. Additionally, we have also recently begun to focus on building relationships with potential distribution partners, to utilize their sales force resources to reach new customers. As a result of these recent changes in our market, sales organization and go-to-market strategies, and with our limited operating history, our ability to forecast our future results of operations and plan for and model future growth is limited and subject to a number of uncertainties.

We have encountered and will continue to encounter risks and uncertainties in developing markets. If our assumptions regarding these risks and uncertainties are incorrect or change in response to developments in the security market, our results of operations and financial results could differ materially from our plans and forecasts. If we are unable to achieve our key objectives, our business and results of operations will be adversely affected, and the fair market value of our common stock could decline.

Our growth prospects and revenue will be adversely affected if our efforts to attract prospective customers and to retain existing customers are not successful.

Our ability to grow our business and generate revenue depends on retaining and expanding our total customer base and increasing services revenue by effectively monetizing value added. We must convince prospective customers of the benefits of our solutions and our existing customers of the continuing value of our solutions. Our ability to attract new customers, retain existing customers, and reach out to new markets depends in large part on our ability to continue to offer leading technologies and products, superior security and trust, and integration capabilities. For instance, in our IoT segment, some of our semiconductors competitors, including Infineon, Microchip, NXP and STMicroelectronics, have developed, and are continuing to develop, secure elements, which puts us at a significant competitive disadvantage.

Failure to protect our intellectual property could substantially harm our business, operating results, and financial condition.

The success of our business depends on our ability to protect and enforce our patents, trade secrets, trademarks, copyrights, and all of our other intellectual property rights, including the silicon intellectual property rights of our semiconductors.

We attempt to protect our intellectual property under patent, trade secret, trademark, and copyright law through a combination of employee, third-party assignment and nondisclosure agreements, other contractual restrictions, technological measures, and other methods. These afford only limited protection and we are still early in the process of securing our intellectual property rights. Despite our efforts to protect our intellectual property rights and trade secrets, unauthorized parties may attempt to copy aspects of our technology, or obtain and use our trade secrets and other confidential information. Moreover, policing our intellectual property rights is difficult and time consuming. We cannot assure you that we would have adequate resources to protect and police our intellectual property rights, and we cannot assure you that the steps we take to do so will always be effective.

We have filed, and may in the future file, patent applications on certain of our innovations. It is possible, however, that these innovations may not be patentable. In addition, given the cost, effort, risks, and downside of obtaining patent protection, including the requirement to ultimately disclose the invention to the public, we may choose not to seek patent protection for some innovations. Furthermore, our patent applications may not issue as granted patents, the scope of the protection gained may be insufficient or an issued patent may be deemed invalid or unenforceable. We also cannot guarantee that any of our present or future patents or other intellectual property rights will not lapse or be invalidated, circumvented, challenged, or abandoned. Neither can we guarantee that our intellectual property rights will provide competitive advantages to us. Our ability to assert our intellectual property rights against potential competitors or to settle current or future disputes could be limited by our relationships with third parties, and any of our pending or future patent applications may not have the scope of coverage originally sought. We cannot guarantee that our intellectual property rights will be enforced in jurisdictions where competition may be intense or where legal protection may be weak. We could lose both the ability to assert our intellectual property rights against, or to license our technology to, others and the ability to collect royalties or other payments.

Litigation or proceedings before governmental authorities and administrative bodies may be necessary in the future to enforce our intellectual property rights, to protect our patent rights, trademarks, trade secrets, and domain names and to determine the validity and scope of the proprietary rights of others. Our efforts to enforce or protect our proprietary rights may be ineffective and could result in substantial costs and diversion of resources and management time, each of which could substantially harm our operating results. Additionally, changes in law may be implemented, or changes in interpretation of such laws may occur, that may affect our ability to protect and enforce our patents and other intellectual property.

Assertions by third parties of infringement or other violation by us of their intellectual property rights could harm our business, operating results, and financial condition.

Third parties may assert that we have infringed, misappropriated, or otherwise violated their copyrights, patents, and other intellectual property rights, and, as we face increasing competition, the possibility of intellectual property rights claims against us grows.

Our ability to provide our services is dependent upon our ability to license intellectual property rights, including to semiconductor designs. Various laws and regulations govern the copyright and other intellectual property rights associated with semiconductor design and cryptographic algorithms. Existing laws and regulations are evolving and subject to different interpretations, and various legislative or regulatory bodies may expand current or enact new laws or regulations. Although we expend significant resources to seek to comply with the statutory, regulatory, and judicial frameworks by, for example, entering into license agreements, we cannot assure you that we are not infringing or violating any third-party intellectual property rights, or that we will not do so in the future.

Moreover, for our semiconductor solutions, we rely on multiple hardware designers, and firmware and software programmers to design our proprietary technologies. Although we make every effort to prevent the incorporation of licenses that would require us to disclose code and/or innovations in our products, we do not exercise complete control over the development efforts of our developers, and we cannot be certain that our developers have not used designs or software that is subject to such licenses or that they will not do so in the future. In the event that portions of our proprietary technology are determined to be subject to licenses that require us to publicly release the affected portions of our semiconductor design and source code, re-engineer a portion of our technologies, or otherwise be limited in the licensing of our technologies, we may be forced to do so, each of which could materially harm our business, operating results, and financial condition.

We derive a significant amount of our revenues each year from a limited number of significant customers.

We derive a significant amount of our revenues each year from a small number of customers. Our business and results of operations are largely dependent upon the success or our significant customers. The loss of any large customer, a decline in the volume of sales to these customers or the deterioration of their financial condition could adversely affect our business, results of operations and financial conditions.

One of our largest customers is CISCO Systems International ("Cisco"). We operate under the terms of a Master Purchase Agreement, dated August 14, 2014. Such agreement defines, among other things:

- the communication process that we shall respect vis a vis forecasting / pricing update, such as determination of price reflecting component prices in effect on the date of shipment to Cisco's authorized contract manufactures ("EMS Provider"), representations and warranties that the product price are, and shall be, no higher than the lowest prices offered by the Company to any customer purchasing the same or lesser total sales or unit volume on an annual basis;
- buffer stock, timing and volume constitution rules, including but not limited to, obligations to make commercially reasonable efforts to conduct capacity and materials planning and management sufficient to meet EMS Provider's forecast at the period of time agreed between WISEKey and EMS Providers,
- list of contract manufacturers to whom we are allowed to take purchase orders and to make deliveries;
- rules of fair treatment in case capacity shortage, that is, an obligation to provide Cisco, EMS Providers and any third party designated by Cisco an allocation of products during its shortage that is no less favorable than that provided to any other customer;
- warranties, including but not limited to, three years warranty period, delivered product having no less than eight remaining weeks of shelf-life, replacement of defected products within two business days in general;
- Epidemic failure rules/treatment. Epidemic failure shall be recognized when a single failure mode in excess of 1% of the product or a multiple failure more in excess of 3% of the product, during any rolling 3-full calendar month period, occurs. If an Epidemic failure happens during the five-year period after the delivery of a product, the Company shall, including but not limited to, notify to Cisco, provide a preliminary plan for problem diagnosis within one business day of the notification, and compensate Cisco for all reasonable costs incurred by Cisco, provide Cisco, EMS Providers and any third party designated by Cisco, subject to the liability exclusions and limitations set forth in the agreement.

Any decline in demand for our IoT products from our clients could have a material adverse effect on the Company's business, results of operations and financial condition.

Our IoT segment is at risk of our clients delaying or withdrawing purchase orders for items where we already committed to the production of these pieces. In these situations, and when sufficient notice is given, we are usually able to adjust our semiconductors production schedules such that the production can be transferred to alternative clients thereby limiting our exposure. However, there can be a short-term impact upon the levels of stock that we hold at any given point in time. As our products have a lengthy development cycle, often being in the region of 18 to 24 months from design-win to delivering the first batch of finished goods, we are not susceptible to losing clients without a lengthy notice period, so there is a very limited risk that we find ourselves holding material amounts of stocks of finished goods that will not be eventually delivered to our clients. The greatest risk is that a client might reduce their production allocations with the Company and, in this instance, we would be required to adapt our purchase requirements accordingly. Most of our raw materials (in particular our wafers) can be redirected to alternative products and so the risk is limited to finished goods. In the event that a client was to significantly reduce demand with a limited lead-time and not place new orders for that product at a later stage, this could lead to some finished goods becoming obsolete, but this risk is considered remote by management. The main risk arising from a decline in demand for our products from one of our top ten clients is that we would need to find new sources of revenue to replace the departing clients.

We depend on our ability to attract new customers and to maintain and grow existing customers, and failure to do so may harm our future revenues and operating results.

Our success depends in large part on our ability to attract new customers ("hunting") and to expand within existing customers ("farming"). The number of new customers and the growth at existing customers in a given period impacts both our short-term and long-term revenues. If WISEKey is unable to successfully attract a sufficient number of new customers, we may be unable to generate revenue growth.

A large amount of investment in sales and marketing and support personnel is required to attract new customers. If we are unable to convince these potential new customers of a need for our products or if we are unable to persuade them of our products' efficacy, we may be unable to achieve growth and there may be a meaningful negative impact on future revenues and operating results.

The use of cryptography is subject to a variety of laws around the world. Unfavorable developments in legislation and regulation may adversely affect our business, operating results, and financial condition.

The use of cryptography is subject to a variety of laws around the world. Government regulation of the internet is evolving and any changes in government regulations relating to the internet or other areas of our business or other unfavorable developments may adversely affect our business, operating results, and financial condition.

For example, the U.S. agency NIST is in the process of selecting post-quantum cryptographic algorithms for all governmental use of cryptography. We depend on their final selection to make our products successful and, should we fail to be able to implement the finally selected algorithm, our ability to serve the U.S. market and by extension the rest of the world may be severely impacted.

Our IoT supply chain depends on third-party suppliers. Failure of one of our suppliers to handle increased demand could impact our ability to take advantage of upside business opportunities.

We outsource several critical functions in our supply chain to third-party suppliers such as the manufacture of our semiconductors. They all have a number of risks that are present in their businesses that could limit their ability to meet increased demands if we see increased orders from our customers. If our suppliers cannot satisfy our demand, we may not be able to meet our customer demands. Also, if our suppliers add higher costs to cover their increased volume, we may see drops in our gross profit margins. Many of these costs are not fixed, even though there may be contracts in place, and may be increased at the discretion of the third-party vendor.

Our agreement with one of our third-party suppliers, Presto Engineering Inc., defines, among other things,

- the list of operational obligations that they shall execute for us. Presto's services include New Production Introduction ("NPI"), such as planning of validation and qualification activities, engineering evaluation of the product and preliminary test solution, and product release to industrial maturity, and Supply Chain Management ("SCM");.
- the On-Time Delivery objectives and rules. Presto is required to provide its SCM service based on agreed targets for On Time Delivery ("OTD"). OTD is defined numerically and it constitute result obligations under French laws, which govern the agreement;
- Their obligations vis a vis our quality process and our security process , including their obligations to be audited on a yearly basis.

Although common in our industry, we do not have agreements with any other of our major third-party suppliers. Rather, the Company provides such suppliers with purchase orders on a quarterly basis which triggers the launch of manufacturing of the Company's products. The Company has weekly discussions and provides the suppliers with 12 month rolling forecasts to allow them to anticipate equipment allocations and raw material supplies. However, since we do not have written agreements with these suppliers, we are subject to the risk that any of these suppliers could terminate their relationship with us, leaving us without critical products, software or other services needed to operate our business.

Our IC products mainly depend on supplies from third-party foundries, and any failure to obtain sufficient foundry capacity from such foundries would significantly delay the shipment of our products.

Our IoT segment is a fabless IC design business and, as such, we do not own any IC fabrication facilities. We currently work with two leading foundries as our main IC fabrication partners and place purchase orders according to our business needs. It is important for us to have a reliable relationship with third-party foundries as well as other future foundry service providers to ensure adequate product supply to respond to customer demand.

We cannot guarantee that our foundry service providers will be able to meet our manufacturing requirements. The ability of our foundry service providers to provide us with foundry services is limited by available capacity. If any of our foundry service providers fails to succeed in their capacity promise, it will not be able to deliver to us ICs as per the Purchase Orders that we have placed to them, which will significantly affect our shipment of our products and solutions. This could in turn result in lost sales and have a material adverse effect on our relationships with our customers and on our business and financial condition. In addition, we do not have a guaranteed level of production capacity from our foundry service providers. We do not have long-term contracts with them, and we source our supplies on a purchase order basis. As a result, we depend on our foundry service providers to allocate to us a portion of its manufacturing capacity sufficient to meet our needs, produce products of acceptable quality and at acceptable final test yields and deliver those products to us on a timely basis and at acceptable prices. If any of our foundry service providers raises its prices or is unable to meet our required capacity for any reason, such as shortages or delays in the shipment of semiconductor equipment or raw materials required to manufacture our ICs, or if our business relationships with any of our foundry service providers deteriorate, we may not be able to obtain the required capacity and would have to seek alternative foundries, which may not be available on commercially reasonable terms, or at all. Moreover, it is possible that other customers of any of our foundry service providers that are larger and/or better financed than we are, or that have long-term contracts with it, may receive preferential treatment in terms of capacity allocation or pricing. In addition, if we do not accurately forecast our capacity needs, any of our foundry service providers may not have available capacity to meet our immediate needs or we may be required to pay higher costs to fulfill those needs, either of which could materially and adversely affect our business, results of operations or financial condition.

Other risks associated with our dependence on third-party foundries include limited control over delivery schedules and quality assurance, lack of capacity in periods of excess demand, unauthorized use of our intellectual property and limited ability to manage inventory and parts. In particular, although we have entered into confidentiality agreements with our third-party foundries for the protection of our intellectual property, they may not protect our intellectual property with the same degree of care as we use to protect our intellectual property. If we fail to properly manage any of these risks, our business and results of operations may be materially and adversely affected.

Moreover, if any of our foundry service providers suffers any damage to its facilities, suspends manufacturing operations, loses benefits under material agreements, experiences power outages or computer virus attacks, lacks sufficient capacity to manufacture our products, encounters financial difficulties, is unable to secure necessary raw materials from its suppliers or suffers any other disruption or reduction in efficiency, we may encounter supply delays or disruptions.

We rely on a limited number of third parties for IC packaging and testing services.

In relation to our IoT segment, fabrication of ICs requires specialized services to process the silicon wafers into ICs by packaging them and to test their proper functioning. We primarily collaborate with a Outsource Semiconductors Assembly and Testing (OSAT) provider for such services, which may expose us to a number of risks, including difficulties in finding alternate suppliers, capacity shortages or delays, lack of control or oversight in timing, quality or costs, and misuse of our intellectual property. If any such problems arise with our packaging and testing partners, we may experience delays in our production and delivery timeline, inadequate quality control of our products or excessive costs and expenses. As a result, our financial condition, results of operations, reputation and business may be adversely affected.

Failure at tape-out or failure to achieve the expected final test yields for our ICs could negatively impact our results of operations.

The tape-out process is a critical milestone in our IoT segment. A tape-out means all the stages in the design and verification process of our ICs have been completed, and the chip design is sent for manufacturing. The tape-out process requires considerable investment in time and resources and close cooperation with the wafer foundry, and repeated failures can significantly increase our costs, lengthen our product development period, and delay our product launch. If the tape-out or testing of a new chip design fails, either as a result of design flaws by our research and development team or problems with production or the testing process by the wafer foundry, we may incur considerable costs and expenses to fix or restart the design process. Such obstacles may decrease our profitability or delay the launch of new products.

Once tape-out is achieved, the IC design is sent for manufacturing, and the final test yield is a measurement of the production success rate. The final test yield is a function of both product design, which is developed by us, and process technology, which typically belongs to a third-party foundry. Low final test yields can result from a product design deficiency or a process technology failure or a combination of both. As such, we may not be able to identify problems causing low final test yields until our product designs go to the manufacturing stage, which may substantially increase our per unit costs and delay the launch of new products.

Changes in regulations or citizen concerns regarding privacy and protection of citizen data, or any failure or appearance of failure to comply with such laws, could diminish the value of our services and cause us to lose customers and revenue.

The regulatory framework for privacy issues worldwide is currently in flux and is likely to remain so for the foreseeable future. Practices regarding the collection, use, storage, transmission, and security of personal information by companies operating over the internet have recently come under increased public scrutiny.

The U.S. government, including the Federal Trade Commission and the Department of Commerce, may continue to review the need for greater regulation over the collection of information concerning consumer behavior on the internet, including regulation aimed at restricting certain targeted advertising practices.

Additionally, the EU may continue to review the need for greater regulation or reform to its existing data protection legal framework, which may result in a greater compliance burden for companies with users in Europe. Various government and consumer agencies also have called for new regulation and changes in industry practices. Our business, including our ability to operate and expand internationally, could be adversely affected if legislation or regulations are adopted, interpreted, or implemented in a manner that is inconsistent with our current business practices and that require changes to these practices, the design of our website, services, features, or our privacy policy. In particular, the success of our business has been, and we expect will continue to be, driven by our ability to responsibly use the personal data that our customers share with us.

Therefore, our business could be harmed by any significant change to applicable laws, regulations, or industry practices regarding the use of our customers' personal data, for example regarding the manner in which disclosures are made and how the express or implied consent of customers for the use of personal data is obtained. Such changes may require us to modify our services and features, possibly in a material manner, and may limit our ability to develop new services and features that make use of the data that our customers voluntarily share with us. In addition, some of our developers or other partners, such as those that help us measure the effectiveness of advertisements, may receive or store information provided by us or by our customers through mobile or web applications integrated with our services. We provide limited information to such third parties based on the scope of services provided to us. However, if these third parties or developers fail to adopt or adhere to adequate data security practices, or in the event of a breach of their networks, our data or our customers' data may be improperly accessed, used, or disclosed.

Cybersecurity incidents, including data security breaches or computer viruses, could harm our business by disrupting our delivery of services, damaging our reputation or exposing us to liability.

We receive, process, store and transmit, often electronically, the data of our customers and others, much of which is confidential. Unauthorized access to our computer systems or stored data could result in the theft, including cyber-theft, or improper disclosure of confidential information, and the deletion or modification of records could cause interruptions in our operations. These cyber-security risks increase when we transmit information from one location to another, including over the Internet or other electronic networks. Despite the security measures we have implemented, our facilities, systems and procedures, and those of our third-party service providers, may be vulnerable to security breaches, acts of vandalism, software viruses, misplaced or lost data, programming or human errors or other similar events which may disrupt our delivery of services or expose the confidential information of our customers and others. Any security breach involving the misappropriation, loss or other unauthorized disclosure or use of confidential information of our customers or others, whether by us or a third party, could subject us to civil and criminal penalties, have a negative impact on our reputation, or expose us to liability to our customers, third parties or government authorities. We are not aware of such breaches or any other material cyber-security risks in our supply chain to date. Any of these developments could have a material adverse effect on our business, results of operations and financial condition.

To mitigate these risks, we comply with one of the highest security standards in our industry: Webtrust, ISO27001 and the "Common Criteria" standard. Compliance with these standards require us to implement, monitor and audit on a yearly basis all the processes where we, or our third-party suppliers, manipulate sensitive data. This includes our supply chain processes and partners which, like us, are audited every year by security experts certified by governmental authorities. In addition, one of our customers, Cisco, also conducts an independent and extensive audit to control our processes and proposes improvements.

Our security processes are piloted by a Global Security Director, under the supervision of a Security Board, which includes the top management of WISEKey. Once a year, the Global Security Director reassesses our cybersecurity risks and proposes to the Security Board a plan of action and budget for the year to come.

The Executive Board Members of WISEKey hold a weekly meeting to discuss all matters including operational matters and risk management, as well as holding regular, wider meetings with the Senior Management of WISEKey. During these meetings, the risks faced by the business and any new matters arising or potential threats identified are discussed. The WISEKey management team also provide updates on their ongoing projects designed to manage these risks, as well as presenting the results of any audits that are being carried out. The full Board are also kept apprised on the results of all audits carried out during the year and are required to decide on strategic decisions such as whether to attain accreditations for the business. The Board and Audit Committee are responsible also for overseeing the annual audit of WISEKey which, while primarily focused on the financials of WISEKey, does also cover certain risks associated with the business.

If our security systems are breached, we may face civil liability, and public perception of our security measures could be diminished, either of which would negatively affect our ability to attract and retain customers.

Techniques used to gain unauthorized access to data and software are constantly evolving, and we may be unable to anticipate or prevent unauthorized access to cryptographic data. Our software services, which are supported by our own systems and those of third parties that we work with, are vulnerable to software bugs, computer viruses, internet worms, break-ins, phishing attacks, attempts to overload servers with denial-of-service, or other attacks and similar disruptions from unauthorized use of our and third-party computer systems, any of which could lead to system interruptions, delays, or shutdowns, causing loss of critical data or the unauthorized access to personal data.

Computer malware, viruses, computer hacking, and phishing attacks have become more prevalent in our industry. WISEKey and WISEKey's systems have been subject to such attacks in the past, albeit they have always been unsuccessful, and further such attempts to compromise our systems' security may occur in the future. Because of our brand of trust and security, we believe that we are a particularly attractive target for such attacks. Though it is difficult to determine what, if any, harm may directly result from any specific interruption or attack, any failure to maintain performance, reliability, security, and availability of our products and technical infrastructure to the satisfaction of our customers may harm our reputation and our ability to retain existing customers and attract new customers. Although we have developed systems and processes that are designed to protect our data and user data, to prevent data loss, to disable undesirable accounts and activities on our platform, and to prevent or detect security breaches, we cannot assure you that such measures will provide absolute security, and we may incur significant costs in protecting against or remediating cyber-attacks.

Additionally, if an actual or perceived breach of security occurs to our systems or a third party's platform, we may face regulatory or civil liability and public perception of our security measures could be diminished, either of which would negatively affect our ability to attract and retain customers, which in turn would harm our efforts to attract and retain advertisers, content providers, and other business partners. We also would be required to expend significant resources to mitigate the breach of security and to address matters related to any such breach. We also may be required to notify regulators about any actual or perceived personal data breach (including the EU Lead Data Protection Authority) as well as the individuals who are affected by the incident within strict time periods.

Any failure, or perceived failure, by us to maintain the security of data relating to our customers, to comply with our posted privacy policy, laws and regulations, rules of self-regulatory organizations, industry standards, and contractual provisions to which we may be bound, could result in the loss of confidence in us, or result in actions against us by governmental entities or others, all of which could result in litigation and financial losses, and could potentially cause us to lose customers, advertisers, and revenues. In Europe, European Data Protection Authorities could impose fines and penalties of up to 4% of annual global turnover or €20 million, whichever is higher, for a personal data breach.

Our semiconductors and software services are highly technical and may contain undetected software bugs or vulnerabilities, which could manifest in ways that could seriously harm our reputation and our business.

Our semiconductors and software services are highly technical and complex and may contain undetected software bugs, hardware errors, and other vulnerabilities. These bugs and errors can manifest in any number of ways in our products, including through diminished performance, security vulnerabilities, malfunctions, or even permanently disabled products.

Some errors in our products may be discovered only after a product has been used by customers and may in some cases be detected only under certain circumstances or after extended use. Any errors, bugs, or other vulnerabilities discovered in our code or back-end after delivery could damage our reputation, drive away customers, allow third parties to manipulate or exploit vulnerabilities.

We also could face claims for product liability, tort, or breach of warranty. Defending a lawsuit, regardless of its merit, is costly and may divert management's attention and seriously harm our reputation and our business. In addition, if our liability insurance coverage proves inadequate or future coverage is unavailable on acceptable terms or at all, our business could be seriously harmed.

Interruptions, delays or discontinuations in service arising from our own systems or from third parties could impair the delivery of our services and harm our business.

We rely on systems housed in our own facilities and upon third parties, including bandwidth providers and third-party "cloud" data storage services, to enable our customers to receive our content in a dependable, timely, and efficient manner. We have experienced and may in the future experience periodic service interruptions and delays involving our own systems and those of third parties that we work with. Both our own facilities and those of third parties are vulnerable to damage or interruption from earthquakes, floods, fires, power loss, telecommunications failures, and similar events. They also are subject to break-ins, sabotage, intentional acts of vandalism, the failure of physical, administrative, technical, and cyber security measures, terrorist acts, natural disasters, human error, the financial insolvency of third parties that we work with, and other unanticipated problems or events. The occurrence of any of these events could result in interruptions in our services and to unauthorized access to, or alteration of, the content and data contained on our systems and that these third parties store and deliver on our behalf.

Any disruption in the services provided by these third parties could materially adversely impact our business reputation, customer relations, and operating results. Upon expiration or termination of any of our agreements with third parties, we may not be able to replace the services provided to us in a timely manner or on terms and conditions, including service levels and cost, that are favorable to us, and a transition from one third party to another could subject us to operational delays and inefficiencies until the transition is complete.

Our business model consists in promoting trust and security, and it depends on trust in our brand. Negative media coverage could adversely affect our brand and any failure to maintain, protect, and enhance our brand would hurt our ability to retain or expand our customer base.

Maintaining, protecting, and enhancing our brand is critical to expanding our customer base, and will depend largely on our ability to continue to develop and provide top-level security. If we do not successfully maintain our brand, our business could be harmed.

Our brand may be impaired by a number of other factors, including a failure to protect the cryptographic keys, data and software of end customers, any failure to keep pace with technological advances on our platform or with our services, a failure to protect our intellectual property rights, or any alleged violations of law, regulations, or public policy. Further, if our partners fail to maintain high standards in the supply chain, or if we partner with supply chain partners that our customers reject, the strength of our brand could be adversely affected.

We have not historically been required to spend considerable resources to establish and maintain our brand. However, if we are unable to maintain the growth rate in our customer base, we may be required to expend greater resources on advertising, marketing, and other brand-building efforts to preserve and enhance brand awareness, which would adversely affect our operating results and may not be effective.

We depend on our IoT customers' ability to sell their products, which that may pose challenges for our ability to forecast or optimize our inventory and sales.

Large IoT orders may depend on the ability of our customer to be awarded significant regional or national contracts. The design of many IoT devices comes with the risk that it may not see the demand that was expected in that market, or the high-volume contracts may be awarded to competing suppliers. Our customers may be bidding against several other suppliers to win a government contract and if they lose the bid, we will not see the results that were originally expected during the forecasting of the opportunity size and profitability. As such, the volume predictions that were used in the pricing negotiations and forecasts may not always be achievable by our customers and may adversely affect our operating results.

We may need to discontinue products and services. During the ramp-down of such products and services, we may experience a negative impact on our sales.

All products have a natural lifecycle that includes the inevitable end-of-life process. During the ramping down of a product, product family, or services there are many ways that our business operations can be challenged. Last-time-buys are a typical way for customers to deal with the end-of-life of a product that is still critical to one of their end products. These kinds of orders show an increase in short term sales but result in the abrupt drop off of revenue from that customer, for that product, after the last time buy is delivered. Discontinuing a product or service also comes with the risk that we may lose that customer for good if we do not have a replacement for the product or if they decide to look at alternative suppliers because of the change in supply.

Financial Risks

WISeKey has entered, and expects to continue to enter, into joint venture agreements and these activities involve risks and uncertainties.

WISeKey has entered, and expects to continue to enter, into joint venture agreements in order to effectively grow its revenue and penetrate certain geographic regions. Entering into joint venture agreements or other similar forms of partnership involves risks and uncertainties, including the risk that the partners that we enter into joint ventures with will not have the market connections that we expect them to bring to the joint venture. Additionally, there is a risk that a given joint venture could fail to satisfy its obligations, which may result in certain liabilities to us for guarantees and other commitments. Further, since we may not exercise control over our current or future joint ventures, we may not be able to require our joint ventures to take the actions that we believe are necessary to implement our business strategy. Additionally, differences in views among joint venture participants may result in delayed decisions or failures to agree on major issues. If any of these difficulties cause any of our joint ventures to deviate from our business strategy, or if this leads any of our joint ventures to fail to attract the customer base that we project it to attract, our results of operations could be materially adversely affected.

WISeKey is exposed to risks associated with acquisitions and investments.

We may in the future make acquisitions of, or investments in, existing companies or existing or new businesses. Acquisitions and investments involve numerous risks that vary depending on their scale and nature, including, but not limited to:

- diversion of management's attention from other operational matters;
- inability to complete proposed transactions as anticipated or at all (and any ensuing obligation to pay a termination fee or other costs and expenses);
- the possibility that the acquired business will not be successfully integrated or that anticipated cost savings, synergies or other benefits will not be realized;
- the acquired business or strategic partnership may lose market acceptance or profitability;
- a decrease in our cash or an increase in our indebtedness, including security interests that may have to be constituted as part of the acquisition indebtedness, may limit our ability to access additional capital when needed;
- failure to commercialize purchased technologies, intellectual property rights or partnered solutions;
- initial dependence on unfamiliar supply chains or relatively small supply partners;
- inability to obtain and protect intellectual property rights in key technologies;
- incurrence of unexpected liabilities; and
- loss of key personnel and clients or customers of acquired businesses.

In addition, if WISeKey is unsuccessful at integrating such acquisitions or the technologies associated with such acquisitions, our revenues and results of operations could be adversely affected. Any integration process may require significant time and resources, and WISeKey may not be able to manage the process successfully. WISeKey may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, including accounting charges. WISeKey may have to pay cash, incur debt or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition. The sale of equity or incurrence of debt to finance any such acquisitions could result in dilution to our shareholders. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

WISeKey has a history of losses and may not achieve profitability in the future.

WISeKey has invested substantial amounts of financial resources so far on its acquisitions, brand technology and market position. As at December 31, 2022, WISeKey had, on a consolidated level, an accumulated cumulative deficit of USD 265,635,281, compared to USD 238,159,600 as at December 31, 2021 and USD 217,819,809 as at December 31, 2020. In the past, we made significant investments in our operations which have not resulted in corresponding revenue growth and, as a result, increased our losses. WISeKey expects to make significant future investments to support the further development and expansion of our business and these investments may not result in increased revenue or growth on a timely basis or at all.

WISeKey may also incur significant losses in the future for a number of reasons, including slowing demand for our products and services, increasing competition, weakness in the software and security industries generally, as well as other risks described herein, and we may encounter unforeseen expenses, difficulties, complications and delays, and other unknown factors. If WISeKey incurs losses in the future, we may not be able to reduce costs effectively because many of our costs are fixed. In addition, to the extent that we reduce variable costs to respond to losses, this may affect our ability to attract customers and grow our revenues. Accordingly, WISeKey may not be able to achieve or maintain profitability and we may continue to incur significant losses in the future.

Certain of the Company's large shareholders, including if acting in concert, may be able to exert significant influence on the Company and their interests may conflict with the interests of its other shareholders.

Our founder, Carlos Moreira, holds nearly 30% of the Company's voting rights as at December 31, 2022. Further, all holders of the Class A Shares represent approximately 29% of the Company's voting rights as at December 31, 2022. Our founder, or if the holders of Class A Shares were to act in concert with each other, the holders of the Class A Shares, would be able to exert significant influence over certain matters, including matters that must be resolved by the general meeting of shareholders, such as the election of members to the board of directors or the declaration of dividends or other distributions. To the extent that the interests of these shareholders may differ from the interests of the Company's other shareholders, the Company's other shareholders may be disadvantaged by any actions that these shareholders may seek to pursue.

The market for and price of Class B Shares and our ADSs may be highly volatile.

There has not been a public market in the United States for our Class B Shares, and the market for the ADS listed on NASDAQ is limited. You may not be able to sell your ADSs quickly or at the market price if trading in the ADSs is limited.

The market price of Class B Shares and our ADSs may be highly volatile and may be affected negatively by events involving us, our competitors, the software and security industry, or the financial markets in general. Furthermore, investors might not be able to resell their Class B Shares and our ADSs at the price at which they were purchased or at a higher price or at all. Factors that could cause this volatility in the market price of Class B Shares and our ADSs include, but are not limited to:

- our operating and financial results;
- future announcements concerning our business;
- changes in revenue or earnings estimates and recommendations by securities analysts;
- changes in our business strategy and operations;
- changes in our senior management or board of directors;
- speculation of the press or the investment community;
- disposals of Class B Shares by shareholders;
- actions of competitors;

- our involvement in acquisitions, strategic alliances or joint ventures;
- regulatory factors;
- arrival and departure of key personnel;
- investment community views on technology stock;
- liquidity of the Class B Shares and our ADSs; and
- general market, economic and political conditions.

In addition, securities markets in general have from time to time, experienced significant price and volume fluctuations. Such fluctuations, as well as the economic environment as a whole, can have a substantial negative effect on the market price of our securities, regardless of our operating results or our financial position. Any such broad market fluctuations may adversely affect the trading price of our securities.

Our securities are traded on more than one market or exchange and this may result in price variations.

Our Class B Shares have been trading on the SIX since March 2016. The ADSs have been listed on NASDAQ since December 2019. Trading in Class B Shares and ADSs, as applicable, on these markets take places in different currencies (U.S. dollars on NASDAQ and Swiss francs on the SIX), and at different times (resulting from different time zones, trading days, and public holidays in the United States and Switzerland). The trading prices of our Class B Shares and ADSs on these two markets may differ due to these and other factors. Any decrease in the price of our Class B Shares on the SIX could cause a decrease in the trading price of the ADSs on NASDAQ, and vice versa.

Future sales or issuances, or the possibility or perception of future sales or issuances, of a substantial number of Shares could cause the market price of our Class B Shares or the ADSs to fall.

The market price of our Class B Shares or ADSs could decline as a result of sales of a large number of Class B Shares in the public market in the future or the possibility or perception that such sales could occur. These sales, or the possibility that these sales may occur, also might make it more difficult for the Company to issue equity securities in the future at a time and price that it deems appropriate.

Further, the Company may choose to raise additional capital by issuing additional Class B Shares, depending on market conditions or strategic considerations. In particular, under our Articles of Association as at December 31, 2022, the board of directors is authorized to issue up to 25,000,000 new Class B Shares out of authorized capital at any time until June 24, 2024 and thereby increase the Company's share capital without further shareholder approval. After June 24, 2024 (and each subsequent two-year period), the shareholders may re-approve this authorization. Further, our Articles of Association provide for a conditional share capital based on which, as at December 31, 2022, the Company is authorized to issue up to 52,100,000 new Class B Shares, corresponding to CHF 2,605,000 in par value. Since April 29, 2022, the date of reference for the last formal recording in the Articles and the commercial register of the Canton of Zug, Switzerland, an aggregate number of 26,040,010 Class B Shares has been issued out of the Company's conditional share capital as of December 31, 2022. As a result, the available conditional share capital of the Company, as at December 31, 2022, amounted to CHF 1,302,999.50, corresponding to the issuance of 26,059,990 Class B Shares. Among other things, the Company's conditional share capital could be used in connection with the issuance of securities that are convertible into Class B Shares. To the extent that additional capital is raised through the issuance of Class B Shares or other securities that are convertible into Class B Shares, the issuance of such securities could dilute the Company's shareholders' interest in the Company.

On February 8, 2018, the Company entered into a Standby Equity Distribution Agreement, as amended on September 28, 2018 (the "SEDA") with YA II PN, Ltd., a fund managed by Yorkville Advisors Global, LLC (collectively referred to as "Yorkville"). Pursuant to the SEDA, the Company has the right, at any time during a five-year period, to request Yorkville, in one or several steps, to subscribe for Class B Shares up to an aggregate subscription amount of CHF 50,000,000. After several drawdowns made by WISEKey under the SEDA in 2019, 2020 and 2021, in the aggregate amount of CHF 4,356,045, the remaining amount available for drawdown is CHF 45,643,955 as at December 31, 2022. As long as a sufficient number of Class B Shares is provided through share lending, WISEKey has the right to make drawdowns under the SEDA at its discretion by requesting Yorkville to subscribe for (if the Class B Shares are issued out of authorized share capital) or purchase (if the Class B Shares are delivered out of treasury) Class B Shares worth up to CHF 5,000,000 each, subject to certain exceptions and limitations (including the exception that a drawdown request by WISEKey shall in no event cause the aggregate number of Class B Shares held by Yorkville to meet or exceed 4.99% of the total number of shares registered with the commercial register of the Canton of Zug). The subscription price for each subscription request of the Company corresponds to 93% of the lowest daily volume-weighted average share price (the "VWAP") of a Class B Share, as traded and quoted on the SIX, over the five trading days following the drawdown request by WISEKey. If the Company elects to exercise its rights under the SEDA, the issuance of Class B Shares would dilute the Company's shareholders' interest in the Company. As at December 31, 2022, the remaining amount available for drawdown by the Company under the SEDA is CHF 45,643,955 (USD 49,375,851 at closing rate) and, as at December 31, 2022, the estimated maximum number of Class B Shares deliverable under the SEDA is 294,477,130 Class B Shares at CHF 0.155 per Class B Share (calculated based on the closing price of a Class B Share on December 30, 2022 of CHF 0.1672 per Class B Share, discounted by 7%). The actual price, at which the Company may drawdown under the SEDA is subject to change, and, therefore, the number of Class B Shares deliverable to Yorkville may vary.

In connection with a convertible loan agreement WISEKey entered into with Crede CG III, Ltd., Hamilton, Bermuda ("Crede") on September 28, 2018 (which matured on October 30, 2020), the Company granted to Crede, on September 28, 2018, 408,247 warrants (the "Crede Warrants") for the acquisition of an equal number of Class B Shares. As a result, the maximum total number of Class B Shares that are issuable under the Crede Warrants as at December 31, 2022 is 408,247 Class B Shares. The Crede Warrants were amended on September 18, 2020 to extend the exercise period and may be exercised by Crede at any time on or before October 29, 2023 at an exercise price per Crede Warrant equal to CHF 3.84 per Class B Share. The Class B Shares issued to Crede in connection with the Crede Warrants would be issued out of the Company's conditional share capital or authorized share capital without triggering the pre-emptive rights of the existing shareholders of the Company. The exercise of Crede Warrants will dilute the Company's shareholders' interests in the Company.

In connection with a second convertible loan, the Company granted to Crede on August 7, 2020, 1,675,885 warrants (the "Second Crede Warrants") for the acquisition of an equal number of Class B Shares. As a result, the maximum total number of Class B Shares that are issuable under the Second Crede Warrants as at December 31, 2022 is 1,675,885 Class B Shares. The Second Crede Warrants may be exercised by Crede at any time on or before September 14, 2023 at an exercise price per warrant equal to CHF 1.375 per Class B Share, as amended. The Class B Shares issued to Crede in connection with the Second Crede Warrants would be issued out of the Company's conditional share capital or authorized share capital without triggering the pre-emptive rights of the existing shareholders of the Company. The exercise of the Second Crede Warrants will dilute the Company's shareholders' interests in the Company.

In connection with, an Agreement for the Issuance and Subscription of Convertible Notes WISEKey entered into with GLOBAL TECH OPPORTUNITIES 8, Grand Cayman, Cayman Islands ("GTO") on December 8, 2020, the Company granted GTO warrants to acquire Class B Shares at an exercise price of the higher of (a) 120% of the 5-trading day VWAP of the Class B Shares on the SIX Swiss Stock Exchange over the 5 trading days immediately preceding the relevant subscription request and (b) CHF 1.50 (the "GTO Warrant Exercise Price"). The number of warrants granted at each tranche subscription was calculated as 15% of the principal amount of each subscription divided by the GTO Warrant Exercise Price. Each warrant agreement has a 5-year exercise period starting on the relevant subscription date. As at December 31, 2022, a total of 1,319,161 warrants (the "GTO Warrants") have been issued for the acquisition of an equal number of Class B Shares. As a result, the maximum total number of Class B Shares that are issuable under the GTO Warrants as at December 31, 2022 is 1,319,161 Class B Shares. The GTO Warrants may be exercised by GTO at any time until the fifth anniversary of their respective grant at the GTO Warrant Exercise Price. The Class B Shares issued to GTO in connection with the GTO Warrants would be issued out of the Company's conditional share capital or authorized share capital without triggering the pre-emptive rights of the existing shareholders of the Company. The exercise of the GTO Warrants will dilute the Company's shareholders' interests in the Company.

On 29 June 2021, WISEKey entered into an Agreement for the Subscription of up to \$22M Convertible Notes (the “L1 Facility”) with L1 Capital Global Opportunities Master Fund (“L1”), as amended on September 27, 2021 and March 3, 2022, pursuant to which L1 committed to grant loans, in several tranches and in the form of convertible notes (the “L1 Convertible Notes”), to WISEKey up to a maximum amount of USD 22,000,000, subject to certain conditions, over a period of 24 months. The L1 Convertible Notes bear interest at a rate of 6% per annum (“L1 Interest”). Subject to a cash redemption right of WISEKey, the L1 Convertible Notes are mandatorily convertible into Class B Shares within a period of 24 months from issuance of the respective L1 Convertible Notes (the “L1 Conversion Period”), extendable under certain conditions by a maximum of 6 months (the “L1 Maximum Conversion Period”). Conversion takes place upon request by L1 during the L1 Conversion Period, but in any case no later than at the expiry of the L1 Maximum Conversion Period. The conversion price applied to the principal amount of the L1 Convertible Notes and accrued interest, converted into CHF at the relevant exchange rate will be (a) for the tranches subscribed under the original agreement, the lower of (i) 95% of the lowest volume weighted average price of Class B Shares on the SIX Swiss Exchange during the five trading days preceding the relevant conversion date and (ii) depending on the tranche, a fixed conversion price ranging from CHF 4 to CHF 7.50, and (b) for the tranches subscribed under the amendment dated September 27, 2021 and March 3, 2022, 90% of the lowest volume weighted average price of Class B Shares on the SIX Swiss Exchange during the ten trading days preceding the relevant conversion date. WISEKey made several loan subscriptions in 2021 and 2022 under the L1 Facility and there is no remaining amount available for loans as at December 31, 2022. In 2021, L1 requested to convert L1 Convertible Notes issued in 2021 for a total amount of USD 13,500,000, resulting in the issuance of 11,858,831 Class B Shares to L1. In 2022, L1 requested to convert L1 Convertible Notes issued in 2021 and 2022 for a total amount of USD 7,100,000, resulting in the issuance of 29,225,645 Class B Shares to L1. The conversion of the subscriptions under the L1 Facility into Class B Shares will dilute the Company's shareholders' interest in the Company. L1 requested to convert some but not all L1 Convertible Notes issued in 2021 and 2022. As at December 31, 2022, L1 Convertible Notes in an aggregate amount of USD 1,400,000 remained unconverted and there is no remaining amount available for loans, therefore, as at December 31, 2022, the estimated maximum number of Class B Shares deliverable under the L1 Facility is 9,670,583 Class B Shares at a conversion price of CHF 0.15 per Class B Share for the tranches subscribed under the amendment dated March 3, 2022 (calculated based on the closing price of a Class B Share on the SIX on December 30, 2022 of CHF 0.1672 discounted by 10%). Note that the actual price at which L1 may convert each tranche under the L1 Facility is subject to change, and, therefore, the number of Class B Shares deliverable to L1 may vary.

In connection with the L1 Facility, the Company granted L1 the option to acquire Class B Shares at an exercise price of the higher of (a) 1.5 times the 5-trading day volume-weighted average price of the WISEKey Class B Share (“WIHN Class B Share”) on the SIX Swiss Stock Exchange immediately preceding the tranche closing date and (b) CHF 5.00 (the “L1 Warrant Exercise Price”). The number of warrants granted at each tranche subscription is calculated as 25% of the principal amount of each tranche divided by the volume-weighted average price of the trading day immediately preceding the tranche closing date. Each warrant agreement has a 3-year exercise period starting on the relevant subscription date. As at December 31, 2022, a total of 7,990,672 warrants (the “L1 Warrants”) for the acquisition of an equal number of Class B Shares. As a result, the maximum total number of Class B Shares that are issuable under the L1 Warrants as at December 31, 2022 is 7,990,672 Class B Shares. The L1 Warrants may be exercised by L1 at any time until the third anniversary of their respective grant at the L1 Warrant Exercise Price.

On 29 June 2021, WISEKey entered into an Agreement for the Subscription of up to \$22M Convertible Notes (the “Anson Facility”) with Anson Investments Master Fund LP (“Anson”), as amended on September 27, 2021, pursuant to which Anson committed to grant loans, in several tranches and in the form of convertible notes (the “Anson Convertible Notes”), to WISEKey up to a maximum amount of USD 22,000,000, subject to certain conditions, over a period of 24 months. The Anson Convertible Notes bear interest at a rate of 6% per annum (“Anson Interest”). Subject to a cash redemption right of WISEKey, the Anson Convertible Notes are mandatorily convertible into Class B Shares within a period of 24 months from issuance of the respective Anson Convertible Notes (the “Anson Conversion Period”), extendable under certain conditions by a maximum of 6 months (the “Anson Maximum Conversion Period”). Conversion takes place upon request by Anson during the Anson Conversion Period, but in any case no later than at the expiry of the Anson Maximum Conversion Period. The conversion price applied to the principal amount of the Anson Convertible Notes and accrued interest, converted into CHF at the relevant ex-change rate will be (a) for the tranches subscribed under the original agreement, the lower of (i) 95% of the lowest volume weighted average price of Class B Shares on the SIX Swiss Exchange during the five trading days preceding the relevant conversion date and (ii), depending on the tranche, a fixed conversion price ranging from CHF 4 to CHF 7.50, and (b) for the tranches subscribed under the amendment dated September 27, 2021, 90% of the lowest volume weighted average price of Class B Shares on the SIX Swiss Exchange during the ten trading days preceding the relevant conversion date. WISEKey made several loan subscriptions in 2021 under the Anson Facility and the remaining amount available for loans as at December 31, 2022 is USD 5,500,000. In 2021, Anson requested to convert Anson Convertible Notes issued in 2021 for a total amount of USD 9,800,000, resulting in the issuance of 8,228,262 Class B Shares to Anson. In 2022, Anson requested to convert Anson Convertible Notes issued in 2021 for a total amount of USD 6,700,000, resulting in the issuance of 14,351,699 Class B Shares to Anson. The conversion of the subscriptions under the Anson Facility into Class B Shares will dilute the Company's shareholders' interest in the Company. As at December 31, 2022, Anson had requested to convert all Anson Convertible Notes issued in 2021, therefore there is no unconverted Anson Convertible Notes. As at December 31, 2022, the remaining amount available for subscription by the Company under the Anson Facility is USD 5,500,000, therefore, as at December 31, 2022, the estimated maximum number of Class B Shares deliverable under the Anson Facility is 37,962,806 Class B Shares at a conversion price of CHF 0.15 per Class B Share for the tranches subscribed under the amendment dated September 27, 2021 (calculated based on the closing price of a Class B Share on the SIX on December 30, 2022 of CHF 0.1672 discounted by 10%). Note that the actual price at which Anson may convert each tranche under the Anson Facility is subject to change, and, therefore, the number of Class B Shares deliverable to Anson may vary.

In connection with the Anson Facility, the Company granted Anson the option to acquire Class B Shares at an exercise price of the higher of (a) 1.5 times the 5-trading day volume-weighted average price of the WIHN Class B Shares on the SIX Swiss Stock Exchange immediately preceding the tranche closing date and (b) CHF 5.00 (the "Anson Warrant Exercise Price"). The number of warrants granted at each tranche subscription is calculated as 25% of the principal amount of each tranche divided by the volume-weighted average price of the trading day immediately preceding the tranche closing date. Each warrant agreement has a 3-year exercise period starting on the relevant subscription date. As at December 31, 2022, a total of 2,821,922 warrants (the "Anson Warrants") for the acquisition of an equal number of Class B Shares. As a result, the maximum total number of Class B Shares that are issuable under the Anson Warrants as at December 31, 2022 is 2,821,922 Class B Shares. The Anson Warrants may be exercised by Anson at any time until the third anniversary of their respective grant at the Anson Warrant Exercise Price. Should the remaining amount available for subscription by the Company under the Anson Facility of USD 5,500,000 be subscribed for, the estimated maximum number of warrants deliverable under the Anson Facility is 7,602,130 for the acquisition of an equal number of Class B Shares. As a result, assuming the Anson Facility is fully subscribed for, the maximum total number of Class B Shares that are issuable under the Anson Facility as at December 31, 2022 is 10,424,052 Class B Shares (the "Total Anson Warrants"). The Class B Shares issuable to Anson in connection with the Total Anson Warrants would be issued out of the Company's conditional share capital or authorized share capital without triggering the pre-emptive rights of the existing shareholders of the Company. The exercise of the Total Anson Warrants will dilute the Company's shareholders' interests in the Company. Note that the actual volume-weighted average price of the trading day immediately preceding the subscription date at each subscription used to calculate the number of warrants granted to Anson is subject to change, and, therefore, the number of Class B Shares deliverable to Anson may vary.

Our financial results may be affected by fluctuations in exchange rates.

Due to the broad scope of our international operations, a portion of our revenue and our expenses are denominated in currencies other than USD, our reporting currency. As a result, our business is exposed to transactional and translational currency exchange risks caused by fluctuations in exchange rates among those different currencies.

The functional currency of most of our operating subsidiaries is the applicable local currency. The translation from the applicable functional currencies into our reporting currency is performed for balance sheet accounts using exchange rates in effect at the balance sheet date, and, for the statement of operations accounts, using average exchange rates prevailing during the relevant period. Functional currency exchange rates for our operating subsidiaries have in the past, and may in the future, fluctuate significantly against the USD. Because we prepare our consolidated financial statements in USD, these fluctuations may have an effect both on our results of operations and on the reported value of our assets, liabilities, revenue and expenses as measured in USD, which in turn may significantly affect reported earnings, either positively or negatively, and the comparability of period-to-period results of operations.

In addition to currency translation risks, we are exposed to currency transaction risks. Currency transaction risk is the risk that the domestic currency value of a future foreign currency denominated cash flow (payments or receipts from a committed or uncommitted contract or credit facility) varies as a direct result of changes in exchange rates. Fluctuations in currencies may adversely impact our ability to compete on a global basis and our results of operations and our financial condition.

Our operating results can vary significantly due to the impairment of goodwill and other tangible and intangible assets due to changes in the business environment.

Our operating results can also vary significantly due to impairments of intangible assets, including goodwill, and other fixed assets. As at December 31, 2022, the value of our goodwill as recorded on our balance sheet was USD 8,316,892 and the value of acquired technologies and other intangible assets was USD 101,476, net of impairment and amortization. Because the market for our products is characterized by rapidly changing technologies, our future cash flows may not support the value of goodwill and other intangibles recorded in our consolidated financial statements. According to U.S. GAAP, we are required to annually test our recorded goodwill and indefinite-lived intangible assets, if any, and to assess the carrying values of other intangible assets when impairment indicators exist. As a result of such tests, we could be required to book impairment charges in our statement of operations if the carrying value is greater than the fair value. The amount of any potential impairment is not predictable.

Factors that could trigger an impairment of such assets include, but are not limited to, the following:

- underperformance relative to projected future operating results;
- negative industry or economic trends, including changes in borrowing rates or weighted average cost of capital;
- applicable tax rates;
- changes in working capital;
- the market multiples utilized in our fair value calculations;
- changes in the manner or use of the acquired assets or the strategy for our overall business; and
- changes in our organization or management reporting structure, which could require greater aggregation or disaggregation in our analysis by reporting unit and potentially alternative methods/ assumptions of estimating fair values.

Any potential future impairment, if required, could have a material adverse effect on our business, financial condition and results of operations.

We may need additional capital in the future and it may not be available on terms favorable to us or at all.

We may require additional capital in the future to do, among other things, the following:

- fund our operations;
- finance investments in equipment and infrastructure needed to maintain our manufacturing capabilities;
- enhance and expand the range of products and services we offer;
- respond to potential strategic opportunities, such as investments, acquisitions and expansions; and
- service or refinance other indebtedness.

Our ability to obtain external financing in the future is subject to a variety of uncertainties, including: (i) our financial condition, results of operations and cash flows, and (ii) general market conditions for financing activities.

The terms of available financing may also restrict our financial and operating flexibility. If adequate funds are not available on acceptable terms, we may be forced to reduce our operations or delay, limit or abandon expansion opportunities. Moreover, even if we are able to continue our operations, the failure to obtain additional financing could have a material adverse effect on our business, financial condition and results of operations.

The Company is a holding company with no direct cash generating operations and relies on its subsidiaries to provide it with funds necessary to pay dividends to shareholders.

The Company is a holding company with no significant assets other than the equity interests in its subsidiaries. The Company's subsidiaries own substantially all the rights to its revenue streams. The Company has no legal obligation to, and may not, declare dividends or other distributions on its shares. The Company's ability to pay dividends to its shareholders depends on the availability of sufficient legally distributable profits from previous years, which depends on the performance of its subsidiaries and their ability to distribute funds to the Company, and/or on the availability of distributable reserves from capital contributions at the Company level, and on the need for shareholder approval.

The ability of a subsidiary to make distributions to the Company could be affected by a claim or other action by a third party, including a creditor, or by laws which regulate the payment of dividends by companies. In addition, the subsidiaries' ability to distribute funds to the Company depends on, among other things, the availability of sufficient legally distributable profit of such subsidiaries. The Company cannot offer any assurance that legally distributable profit or reserves from capital contributions will be available in any given financial year.

Even if there is sufficient legally distributable profit or reserves from capital contributions available, the Company may not be able to pay a dividend or distribution of reserves from capital contributions for a variety of reasons. Payment of future dividends and other distributions will depend on our liquidity and cash flow generation, financial condition and other factors, including regulatory and liquidity requirements, as well as tax and other legal considerations.

Legal Risks

We are subject to anti-takeover provisions.

Our Articles and Swiss law contain provisions that could prevent or delay an acquisition of the Company by means of a tender offer, a proxy contest or otherwise, that is opposed to by our Board. These provisions may also adversely affect prevailing market prices for our Class B Shares and our ADSs. Even in the absence of a takeover attempt, these provisions may adversely affect the market price of our common stock if they are viewed as discouraging takeover attempts. These provisions provide, among other things:

- an opting-out from the obligation of an acquirer of Shares to make a public offer pursuant to article 135 and 163 of the Swiss Financial Market Infrastructure Act, including its implementing directives, circulars and other regulations (the "FMIA");
- that the share capital is divided into different classes of shares, of which only Class B Shares are listed on the SIX, whereas Class A Shares are not listed and tradable;
- that the Board is currently authorized, at any time until June 24, 2024, to issue up to 25,000,000 new Class B Shares and to limit or withdraw the pre-emptive rights of existing shareholders in various circumstances;
- that any shareholder who is entitled to propose any business or to nominate a person or persons for election as member of the Board at an annual meeting may only do so if advance notice is given to the Company;
- that a merger or demerger transaction requires the affirmative vote of the holders of at least two-thirds of voting rights and an absolute majority of the par value of the shares, each as represented (in person or by proxy) at the general meeting of shareholders and the possibility of a so-called "cash-out" or "squeeze-out" merger if the acquirer controls 90% of the outstanding shares entitled to vote at a general meeting of shareholders; and
- that any action required or permitted to be taken by the holders of shares must be taken at a duly called annual or extraordinary general meeting of shareholders of the Company.

Each Class A Share and each Class B Share has one vote despite the difference in par value

Each Class A Share and each Class B Share carries one vote per share but our Class A Shares have a lower par value (CHF 0.01 per share) than our Class B Shares (CHF 0.05 per share). This means that, relative to their respective per share contribution to the Company's capital, the holders of our Class A Shares have a greater relative per share voting power than the holders of our Class B Shares for matters that require approval on the basis of a specified majority of shares present at the shareholders meeting.

However, to the extent shareholder resolutions require as the relevant majority standard a majority of the par value of the shares present at the meeting, Class A Shares as a class have less votes than Class B Shares as a class (as the Class B Shares have a par value of CHF 0.05 per Class B Share as compared to CHF 0.01 per Class A Share). The majority of par value standard for approval of resolutions applies (i) to shareholder resolutions on certain specific matters (see *Item 10B - Memorandum and Articles of Association - Dual Voting Rights*) and (ii) to the extent that Swiss corporate law requires that a shareholder resolution be adopted with a majority of (A) two-thirds of the voting rights attached to, and (B) the absolute majority of the par value of, the shares, each as represented at the relevant meeting (see also *Item 10B-Memorandum and Articles of Association - Voting Requirements*).

Assuming a total of approximately 140.3 million of our shares are issued (in line with the commercial register of the Canton of Zug as at December 31, 2022), of which approximately 40.0 million are Class A Shares and approximately 100.3 million are Class B Shares, the Class A Shares as a class contribute approximately 7.4% of the aggregate par value of the Company, have 28.5% of the total votes for matters that require approval on the basis of a specified majority of the number of shares present or represented at the shareholders meeting, but 7.4% of the total votes for matters that require approval on the basis of a specified majority of the par value of the shares present at the shareholders meeting. Assuming the same total of approximately 140.3 million of our shares are issued, of which approximately 40.0 million are Class A Shares and approximately 100.3 million are Class B Shares, Class B Shares as a class contribute 92.6% of the aggregate par value of the Company, have 71.5% of the total votes for matters that require approval on the basis of a specified majority of the number of shares present or represented at the shareholders meeting, but 92.6% of the total votes for matters that require approval on the basis of a specified majority of the par value of the shares present at the shareholders meeting.

A change in tax laws, treaties or regulations, or their interpretation, of any country in which we operate, including tax rules limiting the deductibility of interest expense, could result in a higher tax rate on our earnings, which could result in a significant negative impact on our earnings and cash flows from operations.

We operate in various jurisdictions. Consequently, we are subject to changes in applicable tax laws, treaties or regulations in the jurisdictions in which we operate, which could include laws or policies directed toward companies organized in jurisdictions with low tax rates. A material change in the tax laws or policies, or their interpretation, of any country in which we have significant operations, or in which we are incorporated or resident, including the limitation of deductibility of interest expense, could result in a higher effective tax rate on our worldwide earnings and such change could be significant to our financial results.

We may become exposed to costly and damaging intellectual property or liability claims, and our product liability may not cover all damages from such claims.

We are exposed to potential intellectual property or product liability claims. We currently have not been involved in any such legal proceedings. However, the current and future use of our products may expose us to such claims. Any claims made against us, regardless of their merit, could be difficult and costly to defend, and could compromise the market acceptance of our products and any prospects for future products. Such legal proceedings could have a material adverse effect on our business, financial condition, or results of operations.

If WISEKey is unable to adequately protect its proprietary technology and intellectual property rights, its business could suffer substantial harm.

Our intellectual property rights are important to our business. We rely on a combination of confidentiality clauses, trade secrets, copyrights and trademarks to protect our intellectual property and know-how. In addition, we have filed a number of applications for patents to protect our technologies and have been granted two patents in Switzerland for the company's verification and authentication of valuable objects on the Internet in connection with technology involving the internet of things ("IoT") when connecting to each other or to the cloud. Further, in connection with the acquisition of WISEKey Semiconductors SAS from Inside Secure SA, we have acquired 39 patent families.

The steps we take to protect our intellectual property may be inadequate. We will not be able to protect our intellectual property if we are unable to enforce our rights or if we do not detect unauthorized use of our intellectual property. Despite our precautions, it may be possible for unauthorized third parties to copy our products and use information that we regard as proprietary to create solutions and services that compete with ours. Some license provisions protecting against unauthorized use, copying, transfer and disclosure of our solutions may be unenforceable under the laws of certain jurisdictions.

We enter into confidentiality and invention assignment agreements with our employees and consultants and enter into confidentiality agreements with the parties with whom we have strategic relationships and business alliances. No assurance can be given that these agreements will be effective in controlling access to our proprietary information. Further, these agreements do not prevent our competitors from independently developing technologies that are substantially equivalent or superior to our solutions. Additionally, we may from time to time be subject to opposition or similar proceedings with respect to applications for registrations of our intellectual property, including but not limited to our trademarks and patent applications. While we aim to acquire adequate protection of our brand through registrations in key markets, occasionally third parties may have already registered or otherwise acquired rights to identical or similar brands for solutions that also address the cybersecurity, authentication or mobile application markets. Additionally, the process of seeking patent protection can be lengthy and expensive. Any of our pending or future patent or trademark applications, whether challenged or not, may not be issued with the scope of the claims we seek, if at all. We currently own 88 individual patents which preserve our technology.

From time to time, we may discover that third parties are infringing, misappropriating or otherwise violating our intellectual property rights. However, policing unauthorized use of our intellectual property and misappropriation of our technology is difficult and we may therefore not always be aware of such unauthorized use or misappropriation. Despite our efforts to protect our intellectual property rights, unauthorized third parties may attempt to use, copy or otherwise obtain and market or distribute our intellectual property rights or technology or otherwise develop solutions with the same or similar functionality as our solutions. If competitors infringe, misappropriate or otherwise misuse our intellectual property rights and we are not adequately protected, or if such competitors are able to develop solutions with the same or similar functionality as ours without infringing our intellectual property, our competitive position and results of operations could be harmed and our legal costs could increase.

WISeKey may incur fines or penalties, damage to its reputation or other adverse consequences if its employees, agents or business partners violate, or are alleged to have violated, anti-bribery, competition or other laws.

WISeKey's internal controls may not always protect us from reckless or criminal acts committed by our employees, agents or business partners that would violate Swiss, U.S. or other laws, including anti-bribery, competition, trade sanctions and regulations and other related laws. Any such improper actions could subject WISeKey to administrative, civil or criminal investigations in the competent jurisdictions, could lead to substantial civil or criminal monetary and non-monetary penalties against WISeKey or our subsidiaries, and could damage our reputation. Even the allegation or appearance of WISeKey's employees, agents or business partners acting improperly or illegally could damage our reputation and result in significant expenditures in investigating and responding to such actions.

We could be subject to litigation that, if not resolved in our favor and not sufficiently insured against, could have a material adverse effect on us.

As WISeKey continues to expand products, partnerships, sales and distribution, the risk of being involved in legal proceedings will invariably increase. While WISeKey has successfully avoided being involved in legal proceedings in the past, it may not be able to do so in the future. Legal proceedings, especially when involving intellectual property rights and product liability, may have material adverse effects on WISeKey's financial condition, results of operations and cash flows.

We process and store personal information, which subjects us to data protection laws and contractual commitments, and our actual or perceived failure to comply with such laws and commitments could harm our business.

The personal information we process is subject to an increasing number of laws regarding privacy and data protection, as well as contractual commitments. Any failure or perceived failure by us to comply with such obligations may result in governmental enforcement actions, fines, or cause our customers to lose trust in us, which could have an adverse effect on our reputation and business.

We incorporated a wholly-owned subsidiary, SEALSQ Corp, under the laws of the British Virgin Islands.

SEALSQ Corp is currently a wholly-owned subsidiary of WISEKey, incorporated under the laws of the British Virgin Islands. This incorporation expands the operating business of WISEKey in a new jurisdiction, in which we are therefore subject to ongoing regulation and associated regulatory risks, including the effects of changes in the laws, regulations, policies, voluntary codes of practice and interpretations. Such movement of businesses to a new subsidiary will require significant time and resources to implement. It may create operational, capital, funding and tax inefficiencies.

WISEKey transferred the ownership to SEALSQ Corp of WISEKey Semiconductors SAS (formerly known as “VaultIC SAS”), a French semiconductor manufacturer and distributor, WISEKey IoT Japan KK, a Japan-based sales subsidiary of WISEKey Semiconductors SAS, and WISEKey Semiconductors, Taiwan Branch, a Taiwan-based sales and support branch of WISEKey Semiconductors SAS, in a share exchange for 7,501,400 of SEALSQ Corp ordinary shares and 1,499,700 of SEALSQ Corp Class F shares. WISEKey and SEALSQ Corp have executed the services agreement or agreements pursuant to which WISEKey will make available to SEALSQ Corp certain resources, including skilled staff, external consultants and advisors with knowledge across multiple domains, and provide services including, but not limited to, sales and marketing, accounting, finance, legal, taxation, business and strategy consulting, public relations, marketing, risk management, information technology and general management. WISEKey will also make available funding to SEALSQ Corp on the basis of an intra-group loan agreement. The development of SEALSQ Corp is intrinsically linked to the commercial activity of WISEKey, more specifically of WISEKey Semiconductors SAS and its subsidiaries. SEALSQ Corp is particularly vulnerable - but not limited to - to all the business and supply risks related to the semiconductor industry, which could materially and adversely affect its financial stability.

SEALSQ Corp filed a Form F-1, a registration statement under the Securities Act of 1933 for the distribution of 1,500,300 ordinary shares to shareholders of WISEKey as a partial spin-off from WISEKey. Such registration statement was declared effective by the SEC on March 29, 2023. The WISEKey shareholders approved the spin-off distribution at an Extraordinary General Meeting on April 27, 2023. The spin-off transaction is expected to be completed on or about May 25, 2023, and remains subject to the applicable approvals and conditions to the transaction being satisfied or waived, including but not limited to, the approval of the listing of SEALSQ’s Ordinary Shares on the Nasdaq Global Market. SEALSQ Corp has applied to list its ordinary shares on the Nasdaq Global Market under the symbol “LAES.” The spin-off distribution is contingent upon the listing of the ordinary shares on the Nasdaq Global Market or another national securities exchange. There can be no assurance that we will be successful in our listing of SEALSQ Corp’s ordinary shares on the Nasdaq Global Market or another national securities exchange. This spin-off distribution of SEALSQ Corp’s ordinary shares by WISEKey is the first public distribution of the ordinary shares, and prior to this distribution, there has been no public market for the ordinary shares. Accordingly, we can provide no assurance as to what the market price of SEALSQ Corp ordinary shares may be or how strong a secondary market for the ordinary shares will develop.

We incorporated a wholly-owned subsidiary, WISESat.Space AG, under the laws Zug, Switzerland.

WISESat.Space AG is a wholly-owned subsidiary of WISEKey. The incorporation of WISESat.Space AG undertakes to simplify our organizational structure for our activities related to space and satellites. Such reorganization could be disruptive to our business, result in significant expense, require regulatory approvals, and fail to result in the intended or expected benefits, any of which could adversely impact our business and results of operations.

WISEKey will have to correctly assess the business-needs in the fields of space and satellites to achieve profitability with WISESat.Space AG, failing which could materially and adversely affect WISEKey by resulting in the loss of the assets invested in WISESat.Space AG.

Risks Related to Our Shares and ADSs

As a foreign private issuer, we are permitted to rely on exemptions from certain corporate governance standards.

As a foreign private issuer, we are permitted to, and we are relying on exemptions from certain NASDAQ corporate governance standards applicable to domestic U.S. issuers. This may afford less protection to holders of our ordinary shares and the ADSs.

We are exempted from certain corporate governance requirements of NASDAQ by virtue of being a foreign private issuer. We are required to provide a brief description of the significant differences between our corporate governance practices and the corporate governance practices required to be followed by domestic U.S. companies listed on NASDAQ. The standards applicable to us are considerably different than the standards applied to domestic U.S. issuers. For instance, we are not required to:

- have a majority of the board be independent (although all of the members of the audit committee must be independent under the U.S. Securities Exchange Act of 1934, as amended, or the "Exchange Act");
- have a compensation committee or a nominating or corporate governance committee consisting entirely of independent directors; or
- have regularly scheduled executive sessions with only independent directors.

We have relied on and intend to continue to rely on some of these exemptions. As a result, you may not be provided with the benefits of certain corporate governance requirements of NASDAQ.

As a foreign private issuer, we are exempt from certain disclosure requirements under the Exchange Act, which may afford less protection to our shareholders and ADS holders than they would enjoy if we were a domestic U.S. company.

As a foreign private issuer, we are exempt from, among other things, the rules prescribing the furnishing and content of proxy statements under the Exchange Act. In addition, our executive officers, directors and principal shareholders are exempt from the reporting and short-swing profit and recovery provisions contained in Section 16 of the Exchange Act. We are also not required under the Exchange Act to file periodic reports and financial statements with the SEC as frequently or as promptly as domestic U.S. companies with securities registered under the Exchange Act. As a result, our shareholders and ADS holders may be afforded less protection than they would under the Exchange Act rules applicable to domestic U.S. companies.

We may lose our foreign private issuer status, which would then require us to comply with the Exchange Act's domestic reporting regime and cause us to incur significant legal, accounting and other expenses.

As a foreign private issuer, we are not required to comply with all of the periodic disclosure and current reporting requirements of the Exchange Act applicable to U.S. domestic issuers. In order to maintain our current status as a foreign private issuer, either (a) a majority of our common shares must be either directly or indirectly owned of record by non-residents of the United States or (b)(i) a majority of our executive officers or directors may not be United States citizens or residents, (ii) more than 50 percent of our assets cannot be located in the United States and (iii) our business must be administered principally outside the United States. These criteria are tested annually. If we lost this status, we would be required to comply with the Exchange Act reporting and other requirements applicable to U.S. domestic issuers, which are more detailed and extensive than the requirements for foreign private issuers. We may also be required to make changes in our corporate governance practices in accordance with various SEC and stock exchange rules. The regulatory and compliance costs to us under U.S. securities laws if we are required to comply with the reporting requirements applicable to a U.S. domestic issuer may be significantly higher than the cost we would incur as a foreign private issuer. As a result, we expect that a loss of foreign private issuer status would increase our legal and financial compliance costs and would make some activities highly time-consuming and costly. We also expect that if we were required to comply with the rules and regulations applicable to U.S. domestic issuers, it would make it more difficult and expensive for us to obtain director and officer liability insurance, and we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These rules and regulations could also make it more difficult for us to attract and retain qualified members of our board of directors.

We are an "emerging growth company", and we cannot be certain if the reduced disclosure requirements applicable to emerging growth companies may make the ADSs less attractive to investors and, as a result, adversely affect the price of the ADSs and result in a less active trading market for the ADSs.

We are an "emerging growth company" as defined in the U.S. Jumpstart Our Business Startups Act of 2012, or the JOBS Act, and we may take advantage of certain exemptions from various reporting requirements that are applicable to other public companies that are not emerging growth companies. For example, we have elected to rely on an exemption from the auditor attestation requirements of Section 404 of the Sarbanes-Oxley Act relating to internal control over financial reporting, and we will not provide such an attestation from our auditors. We may avail ourselves of these disclosure exemptions until we are no longer an emerging growth company. We cannot predict whether investors will find the ADSs less attractive because of our reliance on some or all of these exemptions. If investors find the ADSs less attractive, it may adversely affect the price of the ADSs and there may be a less active trading market for the ADSs.

We will cease to be an emerging growth company upon the earliest of:

- the last day of the fiscal year during which we have total annual gross revenues of USD 1,070,000,000 (as such amount is indexed for inflation every five years by the United States Securities and Exchange Commission, or SEC) or more;
- the last day of our fiscal year following the fifth anniversary of the completion of our first sale of common equity securities pursuant to an effective registration statement under the Securities Act;
- the date on which we have, during the previous three-year period, issued more than USD 1,070,000,000 in non-convertible debt; or
- the date on which we are deemed to be a "large accelerated filer", as defined in Rule 12b-2 of the Exchange Act, which would occur if the market value of our ordinary shares and ADSs that are held by non-affiliates exceeds USD700,000,000 as of the last day of our most recently-completed second fiscal quarter.

In addition, under the JOBS Act, emerging growth companies can delay adopting new or revised accounting standards issued subsequent to the enactment of the JOBS Act until such time as those standards apply to private companies. Depending on the circumstances, we may or may not take advantage of the extended transition period under Section 7(a)(2)(B) of the Securities Act for complying with new or revised accounting standards and therefore our financial statements may not be comparable to companies that comply with public company effective dates.

The requirements of being a public company may strain our resources and distract our management.

We are required to comply with various regulatory and reporting requirements, including those required by the SEC. Complying with these reporting and other regulatory requirements will be time-consuming and will result in increased costs to us, either or both of which could have a negative effect on our business, financial condition and results of operations.

As a public company, we are (subject to certain exceptions) subject to the reporting requirements of the Exchange Act and the other rules and regulations of the SEC, including the Sarbanes-Oxley Act and the listing and other requirements of NASDAQ. These requirements may place a strain on our systems and resources. The Exchange Act requires that we file annual and current reports with respect to our business and financial performance. The Sarbanes-Oxley Act requires that we maintain disclosure controls and procedures and internal control over financial reporting. To improve the effectiveness of our disclosure controls and procedures and our internal control over financial reporting, we need to commit significant resources and provide additional management oversight. We are implementing additional procedures and processes for the purpose of addressing the U.S. standards and requirements applicable to public companies. These activities may divert management's attention from other business concerns and we will incur significant legal, accounting and other expenses that we did not have prior to the listing on NASDAQ, which could have a material adverse effect on our business, financial condition and results of operations.

We have never paid dividends on our share capital, and we do not anticipate paying cash dividends in the foreseeable future.

We have never declared or paid cash dividends on our share capital. We do not anticipate paying cash dividends on our shares in the foreseeable future. We currently intend to retain all available funds and any future earnings to fund the development and growth of our business. Any future determination to declare cash dividends will be made at the discretion of our board of directors, subject to compliance with applicable laws and covenants under current or future credit facilities, which may restrict or limit our ability to pay dividends and will depend on our financial condition, operating results, capital requirements, distributable profits and/or distributable reserves from capital contributions, general business conditions and other factors that our board of directors may deem relevant. As a result, capital appreciation, if any, of our securities will be your sole source of gain for the foreseeable future.

ADS holders may not be entitled to a jury trial with respect to claims arising under the deposit agreement, which could result in less favorable outcomes to the plaintiffs in any such action.

The deposit agreement governing the ADSs representing our Class B Shares provides that, to the fullest extent permitted by applicable law, ADSs holders waive the right to a jury trial of any claim they may have against us or the depositary arising out of or relating to our Class B Shares, the ADSs or the deposit agreement, including any claim under the U.S. federal securities laws. The waiver to right to a jury trial of the deposit agreement is not intended to be deemed a waiver by any holder or beneficial owner of ADSs of our or the depositary's compliance with the U.S. federal securities laws and the rules and regulations promulgated thereunder.

If we or the depositary oppose a jury trial demand based on the waiver, the court would determine whether the waiver was enforceable based on the facts and circumstances of that case in accordance with the applicable state and federal law. The enforceability of a contractual pre-dispute jury trial waiver in connection with claims arising under the federal securities laws has not been finally adjudicated by the United States Supreme Court. However, we believe that a contractual pre-dispute jury trial waiver provision is generally enforceable, including under the laws of the State of New York, which govern the deposit agreement. In determining whether to enforce a contractual pre-dispute jury trial waiver provision, courts will generally consider whether a party knowingly, intelligently and voluntarily waived the right to a jury trial. We believe that this is the case with respect to the deposit agreement and the ADSs. It is advisable that you consult legal counsel regarding the jury waiver provision before investing in the ADSs.

If you or any other holders or beneficial owners of ADSs bring a claim against us or the depositary in connection with matters arising under the deposit agreement or the ADSs, including claims under federal securities laws, you or such other holder or beneficial owner may not be entitled to a jury trial with respect to such claims, which may have the effect of limiting and discouraging lawsuits against us and/or the depositary. If a lawsuit is brought against us and/or the depositary under the deposit agreement, it may be heard only by a judge or justice of the applicable trial court, which would be conducted according to different civil procedures and may result in different outcome than a trial by jury would have had, including results that could be less favorable to the plaintiffs in any such action.

Nevertheless, if this jury trial waiver is not permitted by applicable law, an action could proceed under the terms of the deposit agreement with a jury trial. No condition, stipulation or provision of the deposit agreement or our ADSs serves as a waiver by any holder or beneficial owner of ADSs or by us or the depositary of compliance with any provision of the U.S. federal securities laws and the rules and regulations promulgated thereunder.

Your voting rights as a holder of our ADSs are limited by the terms of the deposit agreement.

You may exercise your voting rights with respect to the ordinary shares underlying your ADSs only in accordance with the provisions of the deposit agreement. Upon receipt of voting instructions from you in the manner set forth in the deposit agreement, the depositary for our ADSs will endeavor to vote your underlying ordinary shares in accordance with these instructions. When a general meeting is convened, you may not receive sufficient notice of a shareholders' meeting to permit you to withdraw your ordinary shares to allow you to cast your vote with respect to any specific matter at the meeting. In addition, the depositary and its agents may not be able to send voting instructions to you or carry out your voting instructions in a timely manner. We will make all reasonable efforts to cause the depositary to extend voting rights to you in a timely manner, but you may not receive the voting materials in time to ensure that you can instruct the depositary to vote your shares. As a result, you may not be able to exercise your right to vote.

The depositary for our ADSs will deem you as having instructed the depositary to vote the Class B Shares underlying your ADSs in accordance with the voting recommendations of the Company's Board of Directors if you do not give timely voting instructions, except in limited circumstances, which could adversely affect your interests.

Under the deposit agreement for our ADSs, if the depositary does not receive your voting instructions in a timely manner, you will nevertheless be deemed as having instructed the depositary to vote the Class B Shares represented by your ADSs in accordance with the voting recommendations of the Company's Board of Directors, unless:

- we have instructed the depositary that we do not wish a proxy to be given;
- we have informed the depositary that there is substantial opposition as to a matter to be voted on at the meeting; or
- a matter to be voted on at the meeting would have a material adverse impact on shareholders.

The effect of this is that, if you fail to give voting instructions to the depositary, you cannot prevent the Class B Shares underlying your ADSs from being voted in accordance with the voting recommendations of the Company's Board of Directors, absent the situations described above, and it may make it more difficult for shareholders to influence our management.

You may be subject to limitations on transfer of your ADSs.

Your ADSs are transferable on the books of the depositary. However, the depositary may close its transfer books at any time or from time to time when it deems expedient in connection with the performance of its duties. In addition, the depositary may refuse to deliver, transfer or register transfers of ADSs generally when our books or the books of the depositary are closed, or at any time if we or the depositary deems it advisable to do so because of any requirement of law or of any government or governmental body, or under any provision of the deposit agreement, or for any other reason.

You may not receive distributions on our Class B Shares or any value for them if it is illegal or impractical to make them available to you as an ADS holder.

The depositary of our ADSs has agreed to pay you the cash dividends or other distributions it or the custodian for the Class B Shares represented by ADSs after deducting its fees and expenses. You will receive these distributions in proportion to the number of our Class B Shares that your ADSs represent. However, the depositary is not responsible for making such payments or distributions if it is unlawful or impractical to make a distribution available to any holders of ADSs. For example, it would be unlawful to make a distribution to a holder of ADSs if it consists of securities that require registration under the Securities Act but that are not properly registered or distributed pursuant to an applicable exemption from registration. The depositary is not responsible for making a distribution available to any holders of ADSs if any government approval or registration required for such distribution cannot be obtained after reasonable efforts made by the depositary. We have no obligation to take any other action to permit the distribution of our ADSs, Class B Shares, rights or anything else to holders of our ADSs. This means that you may not receive the distributions we make on our Class B Shares or any value for them if it is illegal or impractical for us to make them available to you as an ADS holder. These restrictions may reduce the value of your ADSs.

The rights accruing to holders of our shares may differ from the rights typically accruing to shareholders of a U.S. corporation.

We are organized under the laws of Switzerland. The rights of holders of Class B Shares and, therefore, certain of the rights of ADSs, are governed by the laws of Switzerland and by our Articles of Association. These rights differ in certain respects from the rights of shareholders in typical U.S. corporations. See the sections entitled "Description of Share Capital and Articles of Association - Differences in Corporate Law" and "Description of Share Capital and Articles of Association - Articles of Association - Other Swiss Law Considerations" for a description of the principal differences between the provisions of Swiss law applicable to us and, for example, the Delaware General Corporation Law relating to shareholders' rights and protections.

Claims of U.S. civil liabilities may not be enforceable against us.

We are incorporated under the laws of Switzerland. Certain of our directors reside outside the United States. As a result, it may not be possible for investors to effect service of process within the United States upon such persons or to enforce judgments obtained in U.S. courts against them or us, including judgments predicated upon the civil liability provisions of the U.S. federal securities laws. The United States and Switzerland do not currently have a treaty providing for recognition and enforcement of judgments (other than arbitration awards) in civil and commercial matters. Consequently, a final judgment for payment given by a court in the United States, whether or not predicated solely upon U.S. securities laws, would not automatically be recognized or enforceable in Switzerland. In addition, uncertainty exists as to whether Swiss courts would entertain original actions brought in Switzerland against us or our directors predicated upon the securities laws of the United States or any state in the United States. Any final and conclusive monetary judgment for a definite sum obtained against us in U.S. courts would be reviewed by the courts of Switzerland. Whether these requirements are met in respect of a judgment based upon the civil liability provisions of the U.S. securities laws, including whether the award of monetary damages under such laws would constitute a penalty, is an issue for the court making such decision. If a Swiss court gives judgment for the sum payable under a U.S. judgment, the Swiss judgment will be enforceable by methods generally available for this purpose. These methods generally permit the Swiss court discretion to prescribe the manner of enforcement. As a result, U.S. investors may not be able to enforce against us or certain of our directors, or certain experts named herein who are residents of Switzerland or countries other than the United States, any judgments obtained in U.S.

If we fail to maintain an effective system of internal control over financial reporting, we may not be able to accurately report our financial results or prevent fraud. As a result, shareholders could lose confidence in our financial and other public reporting, which would harm our business and the trading price of ADSs or our Class B Shares.

Effective internal controls over financial reporting are necessary for us to provide reliable financial reports and, together with adequate disclosure controls and procedures, are designed to prevent fraud. Any failure to implement required new or improved controls, or difficulties encountered in their implementation could cause us to fail to meet our reporting obligations. Inadequate internal controls could cause investors to lose confidence in our reported financial information, which could have a negative effect on the trading price of our ADSs or our Class B Shares.

Management will be required to assess the effectiveness of our internal controls annually. However, for as long as we are an "emerging growth company", our independent registered public accounting firm will not be required to attest to the effectiveness of our internal controls over financial reporting. An independent assessment of the effectiveness of our internal controls could detect problems that our management's assessment might not. Undetected material weaknesses in our internal controls could lead to financial statement restatements requiring us to incur the expense of remediation and could also result in an adverse reaction in the financial markets due to a loss of confidence in the reliability of our financial statements.

If securities or industry analysts do not publish research, or publish inaccurate or unfavorable research, about our business, the price of our ADSs or our Class B Shares and their respective trading volumes could decline.

The trading market for our ADSs and our Class B Shares depends in part on the research and reports that securities or industry analysts publish about us or our business. Since we have not undertaken an initial public offering of ADSs in connection with the listing of our ADSs on NASDAQ, we do not anticipate that many or any industry analysts in the United States will publish such research and reports in the United States about our Class B Shares or our ADSs. If no or too few securities or industry analysts commence or continue coverage on us, the trading price for our ADSs and our Class B Shares could be affected. If one or more of the analysts who may eventually cover us downgrade our ADSs or our Class B Shares or publish inaccurate or unfavorable research about our business, the trading price of our ADSs or our Class B Shares would likely decline. If one or more of these analysts cease coverage of us or fail to publish reports on us regularly, demand for our ADSs or Class B Shares could decrease, which might cause the price of such securities and their respective trading volumes to decline.