Memo

TO	Customers	DATE	28-3-2023
FROM	Bob Hulsebosch	EMAIL	Bob.Hulsebosch@inverid.com
CONCERNING	Certifications ReadID	CONFIDENTIALITY	Public

Inverid privacy & trust certificates – from basic to world class

Both customers and users of ReadID trust us with very personal and privacy sensitive information. Inverid has the responsibility to not only *be* secure, but also to *show that we are* secure. We do this via certifications, granted by independent auditors. Customers can rely on these certifications, saving costs and overhead associated with doing their own due diligence and audits on our information security.

Since 2018 we are ISO/IEC 27001 certified, which can be considered as a baseline or 'hygiene' information security certification. For Inverid having more than ISO/IEC 27001 is a differentiator: it creates a competitive edge to our products and assures our customers that we see the security of their information as a top priority for our business. Therefore, we extended this baseline security with several additional certifications. We now have:

1. ISO/IEC 27001 – Information security management
2. ISO/IEC 27701 – Privacy management
3. eIDAS module for Qualified Trust Service Providers
4. eIDAS electronic identification at assurance level High
5. Service Organization Control 2 (SOC2) Type 2 assurance
6. Cyber Essentials cyber security
7. Web content accessibility guidelines WCAG 2.1 level A and AA

Especially the module certification for Qualified Trust Service Provider we are very proud of; to the best of knowledge *we are the first and the only technology provider in the identity verification industry with a certified automated solution*. All our certification have been assessed by the well-known and accredited German/Austrian auditor TÜV.

WE ARE THE FIRST AND THE ONLY TECHNOLOGY PROVIDER IN THE IDENTITY VERIFICATION INDUSTRY WITH A CERTIFIED AUTOMATED SOLUTION FOR QUALIFIED TRUST SERVICE PROVIDERS

Obviously, both eIDAS certifications are not only relevant for trust service or electronic identity providers. For all organisations that need to prove the identity of their end-users, these certifications allow them to do so with ReadID in a proven secure and trustworthy manner.

This memo describes the certifications Inverid currently holds and their benefits for our customers.

ISO/IEC 27001 – Information Security Management

Inverid's ISO/IEC 27001 certification certifies that we have an accurate Information Security Management System (ISMS) in place. That means that we:

- Systematically examine the organisation's information security risks, taking into account the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

The scope of Inverid's ISMS concerns "*Security and privacy in the development, sales, support and service of software products for digital identity*". It enables us to manage the security of our assets such as the personal data read from identity documents and the ReadID software. Included in the scope are the offices in The Netherlands and the UK.

Our Statement of Applicability (SoA) covers all information security controls outlined in Annex A of ISO/IEC 27001. The SoA allows us to justify our information security controls and prove that our defences are implemented in line with an ISO 27001-compliant risk assessment. An independent auditor verifies if the controls are sufficient and properly implemented and managed.

The audit consists of a preliminary review of the ISMS documentation (stage 1) and a more detailed and formal compliance audit (stage 2). In the latter stage, the auditor seeks evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation. Ongoing surveillance activities involve follow-up reviews or audits to assure that our organisation remains in compliance with the standard. Inverid is ISO/IEC 27001 certified since February 2018.

ISO/IEC 27001 INSPIRES CUSTOMER CONFIDENCE AND PROVIDES A SOLID BASIS FOR BUSINESS DEVELOPMENT

ISO/IEC 27001 should be considered as a good practice framework for information security and hygiene factor for customers that want to business with Inverid ReadID and not so much as a competitive differentiator.

For ReadID customers it demonstrates that we have implemented all baseline security controls and provides a solid basis for further business. A necessity for using any security-related service from any provider.

ISO/IEC 27701 – Privacy Management

Whereas the ISO/IEC 27001 certificate provides a baseline security for our ReadID customers, our ISO/IEC 27701 certificate brings it to a next level by adding data privacy specific extensions to it. ISO/IEC 27701 is relatively new and much less common than ISO 27001. ISO/IEC 27701 differentiates ReadID and underlines our continuous efforts to ensure trusted identity verification.

Privacy is a key aspect of our product ReadID, as our solutions have access to many millions of identity documents. We take our responsibility for the privacy of the holders of these documents very seriously.

Inverid's ISO/IEC 27701 certification demonstrates that we have established and implemented an effective Privacy Information Management System extending our ISO/IEC 27001 Information Security Management System. This means that we have all the required security and privacy controls in place to securely process personal data as a controller as well as a processor.

OUR NEW ISO/IEC 27701 PRIVACY CERTIFICATE UNDERLINES OUR CONTINUOUS EFFORTS TO ENSURE TRUSTED IDENTITY VERIFICATION

Privacy controls are laid down in our personal data processing policy and include, for example, encryption of all data in transit and at rest, strict rules on data retention, and comprehensive logging and monitoring. For customers in the European Economic Area all data will be processed on servers within that area. These controls reduce risk to the privacy rights of individuals, to our own organisation and our customers.

ISO/IEC 27701 helps Inverid to be compliant with the European General Data Protection Regulation (GDPR). Please note that, contrary as sometimes claimed, GDPR-specific certifications that demonstrate compliance directly do not exist. Inverid was ISO/IEC 27701 certified in January 2021 by TÜV Trust IT. Recertification takes place every three year with annual surveillance audits in between. This assures our customers that our commitment to maintaining confidentiality, integrity, availability, and privacy of their data is ongoing and will be further evaluated by independent auditors.

For European ReadID customers our ISO/IEC 27701 certificate supports them in achieving their required GDPR compliancy efforts too.

eIDAS module certification for Qualified Trust Service Providers

eIDAS 910/2014 is an EU regulation that establishes trust in electronic transactions between individuals, organisations and government entities across European Member States. Its two core stones are *electronic identification* and *digital signatures*. The module certification is about the latter: it specifies rules for trust services to simplify and standardise digital signatures across Europe. Inverid provides identity data and document verification services for qualified trust service providers operating under the eIDAS regulation. 'Qualified' is the highest trust level, a digital signature at a qualified level is legally equivalent to a wet signature. For these services Inverid has been certified as being compliant with applicable eIDAS requirements as well as relevant applicable ETSI EN 319 401 and ETSI EN 319 411-1/2 standards for qualified trust service providers issuing qualified certificates.

Our practices for remote identity data and document verification with ReadID SaaS with SDK and ReadID Ready are described in our so-called Trust Service Practice Statements. As required by the eIDAS regulation, these are publicly available on the inverid.com website. Moreover, they describe the security of the interfacing with qualified trust service providers and optional facial verification providers. For Inverid this offers flexibility to do business with various qualified trust service providers and facial verification providers without having to recertify.

Inverid's Trust Service Practice Statements for ReadID address our controls that relate to operations and compliance, as outlined by ETSI in relation to availability, security, processing integrity, confidentiality and privacy. These statements are intended to meet the needs of a broad range of customers that need detailed information and assurance about the controls in place and their effectiveness.

We have been certified by TÜV Trust IT since February 2021. TÜV Trust IT is an accredited conformity assessment body for the assessment and certification of qualified trust service providers acting under eIDAS. Trust service providers are regulated by a national supervisory body. Being a module service provider for them means that Inverid is indirectly supervised by the national authority as well. This provides additional assurance that we provide the highest of level of security for our identity verification services.

BEING COMPLIANT WITH THE EIDAS REGULATION ENABLES INNOVALOR TO OFFER CUSTOMERS AN INCREASED CONFIDENCE IN OUR SERVICES AND TAKES AWAY A SUBSTANTIAL PART OF THEIR AUDIT RESPONSIBILITY

This certification is not only of value to qualified trust service providers, but also shows to other customers that ReadID fulfils the information security requirements of this highest level of identity verification.

For qualified service providers that use ReadID our certification takes away audit costs; only their own parts of the qualified service provisioning will need to be audited. The customer's auditors shall rely on the Inverid eIDAS module certification.

As our eIDAS module certificates will be renewed every two year, ongoing compliance and improvement is ensured.

eIDAS eID module certification for assurance level High

The eIDAS 910/2014 regulation establishes trust in electronic transactions between individuals, organisations and government entities across European Member States. Next to digital signatures, it specifies rules for electronic identification to simplify and standardise electronic identities (eIDs), i.e., authentication solutions, across Europe. Inverid's ReadID provides identity data and document verification services for electronic identity providers that issue eIDs under eIDAS. More specific, with ReadID the electronic identity provider obtains authentic identity data from an official identity document that it can use during the registration process of a user applying for an authentication solution at the highest assurance level. For this eID module, Inverid's ReadID services have been assessed by TUV Trust IT to be compliant with assurance level High as specified in eIDAS 2015/1502 implementing regulation (since February 2021).

Compared to Know Your Customer (KYC) and authentication practices in the financial sector that are typically on an eIDAS Substantial level, ReadID is therefore audited *to be trusted at a higher level than Substantial*.

INVERID'S EIDAS eID MODULE CERTIFICATION HELPS CUSTOMERS TO COMPLY WITH SECTOR-SPECIFIC IDENTIFICATION AND AUTHENTICATION REQUIREMENTS UNDER LEGISLATIONS SUCH AS EIDAS, KYC, AML AND PSD2

Our eIDAS conformity assessment helps our customers in the financial sector to show compliance with KYC requirements under the Anti-Money Laundering Directive (AML) and to guarantee the highest level authentication requirements of user in the context of the revised Payment Services Directive (PSD2).

SOC2 type 2 assurance report

Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is widely recognized as a gold standard for data security and requires companies to establish and follow strict information security policies and procedures. This means that Inverid's security system and controls adhere to applicable trust services criteria that customers demand for regulatory compliance and that need detailed information and assurance about the specific controls in place. The assurance is important for Inverid as well as its customers as the ReadID software product of Inverid securely handles large amounts of personal data. Customers need to be able to trust Inverid to do so with utmost care.

> *CUSTOMERS CAN USE THE SOC2 TYPE 2 REPORT TO ASSURE THAT INVERID HAS SIGNIFICANT PROCESSES AND SECURITY MEASURES IN PLACE TO PROTECT USER DATA AND PRIVACY*

Our SOC2 assessment together with our earlier eIDAS certifications proves an unequalled trustworthiness of both our ReadID technology and the company throughout our processes.

The SOC2 assessment was conducted in parallel with the eIDAS audits by Hungarian audit firm Crowe FST Audit Ltd.

Cyber Essentials

Inverid's Cyber Essentials certification helps us to guard against the most common cyber threats and demonstrate our commitment to cyber security.

Cyber Essentials is an effective, UK government backed scheme that helps us to protect our services and customer data against a whole range of the most common cyber attacks.

Since 2023, Inverid has both levels of certification: Cyber Essentials and Cyber Essentials Plus.

WCAG 2.1

Web or digital accessibility is a way of designing websites or mobile applications so that everyone, including people with disabilities, can use them as easily as possible.

WCAG 2.1 is the most recent and relevant accessibility standard for becoming compliant with EU legislation. WCAG 2.1 covers a wide range of recommendations for making web content and mobile apps more accessible. Following these guidelines will make content more accessible to a wider range of people with disabilities, including accommodations for blindness and low vision, deafness and hearing loss, limited movement, speech disabilities, photosensitivity, and combinations of these, and some accommodation for learning disabilities and cognitive limitations; but will not address every user need for people with these disabilities.

As many of our customers have to comply to WCAG 2.1, so does Inverid for its whole portfolio of ReadID offerings such as UI SDK and Ready. Regarding the UI SDK, customers have the ability to partially implement their own WCAG solutions. For other screens and ReadID Ready, Inverid provides proper WCAG solutions at level A and AA.

In the beginning of 2023, ReadID's WCAG 2.1 level A and AA compliancy has been assessed by Accessibility, an independent and accredited accessibility assessment foundation.