CERTUS™ KSI BLOCKCHAIN TECHNOLOGY
SETTING THE STANDARD FOR IMMUTABLE DOCUMENT PROTECTION

CERTUS™ is a novel digital solution that enables document issuers to secure sensitive paper-based and digital documents and credentials with a secure QR-code marking inserted into the credential. The tamper proof technology behind the solution enables credential holders to secure lifelong proof of the validity and authenticity of their credentials. Any third-party verifiers like employers, government officials, auditors, etc. have a very simple, reliable and cost-effective means to carry out independent verification without having to revert to the original issuing authority.

CERTUS™ is backed by the industrially proven KSI, keyless signature infrastructure, blockchain technology. KSI is a method and a globally distributed network infrastructure for the issuance and verification of KSI signatures.

The KSI blockchain was invented in the late 1990s/early 2000s by Estonian cryptographers. The first patent was filed in 2002 and it was launched in early 2008 in an initial pilot for the Estonian Government. Since 2012, all transactions between different databases of the various Estonian administrations are secured via the KSI blockchain. The technology has been accredited by three major governments for deployment on government networks and secures billions of documents, not only for the Estonian government but also for public and private entities around the world including the North Atlantic Treaty Organization (NATO), the U.S. Department of Defense, Lockheed Martin, Boeing and Ericsson.

The KSI blockchain has the following unique properties that make it the logical, pragmatic and reliable choice for document issuers:

- Application agnostic
- No data sharing/exposure
- Full scalability (10^{12}/s)
- Settlement time of 1 second
- Public trust anchor
- No electricity consumption
- No cryptocurrency
- Quantum Proof
- Fully interoperable
- Running 24/7 since 2008

CERTUS™ QR Code

When generating a secure digital or paper document, the unique and sensitive dataset of the document is embedded in a secure QR code (the secure mark) which is applied to each document/credential. The QR code contains two parts:

- **The unique and verifiable data** to be protected (which does not need to be encrypted);
- **A cryptographic signature**, which acts as a mathematically indisputable cryptographic link between the data to be protected and the cryptographic

ABOUT SICPA

SICPA is a leading global provider of secured authentication, identification and traceability solutions and services and a long-trusted advisor to governments, central banks, high security printers and industry. Founded in 1927, headquartered in Switzerland and operating on five continents, SICPA's mission is to Enable Trust through constant innovation. Every day, governments, companies, and millions of people rely on us to protect the integrity and value of their currency, personal identity, documents, products, and brands.

seal, secured by KSI blockchain. It is the heart of the security mechanism which protects the integrity of the sensitive data, making the QR code content impossible to tamper with or forge.

KSI Blockchain vs PKI Timestamping

Unlike traditional digital signature approaches, e.g. Public Key Infrastructure (PKI), that depend on asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain.

The KSI blockchain overcomes two major weaknesses of traditional blockchains, making it usable at industrial scale:

- **Scalability**: One of the most significant challenges with traditional blockchain approaches is scalability – they scale at O(n) complexity i.e. they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) complexity – it grows linearly with time and independently from the number of transactions.
- **Settlement time**: In contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second.

Property	KSI Blockchain	PKI Timestamping
Key Management	No keys are needed for the signature verification -- NO shared secret	Relies on the trustworthy key management -- secrets can be exposed.
Trust Model	Independent mathematical verification based on widely witnessed evidence, including print media	Reliance on trusted service provider and validity of Certificate Revocation lists
Lifetime / expiration	Unlimited, KSI Signatures do not expire	Limited, expiration typically within 3-5 years
Quantum vulnerability	Not vulnerable (relies only on hash cryptography)	Vulnerable
Legal enforcement	Qualified eIDAS trust service	Qualified eIDAS trust service

SICPA
8000 Research Way
Springfield, VA 22153
USA

Tel. +1 703 455 8050
Fax. +1 703 455 4518

securitysolutionsUS@
sicpa.com
www.sicpa.com

Technical information in this document is subject to change without notice.
For additional information, please contact your sales or technical representative.
© 2021, SICPA, USA

CERTUS™ is a trademark of SICPA HOLDING SA, registered (or pending registration) in Switzerland and other countries or otherwise protected by law. All material in these pages, including text, layout, presentation, logos, icons, photos and all other artwork including any derivative work, is the intellectual property of SICPA (for the purpose of this document the word "SICPA" shall mean SICPA HOLDING SA or any of its parent or affiliate companies) unless otherwise stated, and is protected by trademark, patent or copyright. No reproduction, derivative, or commercial use of any material is authorized with-out the prior express written permission by SICPA. Information contained in, or derived from, these pages shall not be used for development, production, marketing of any product or service, or for any other purpose, without the express prior written permission of SICPA.