

CERTUS®

THE TRUSTED
SOLUTION
FOR DIGITAL
AND PRINTED
DOCUMENT
CERTIFICATION

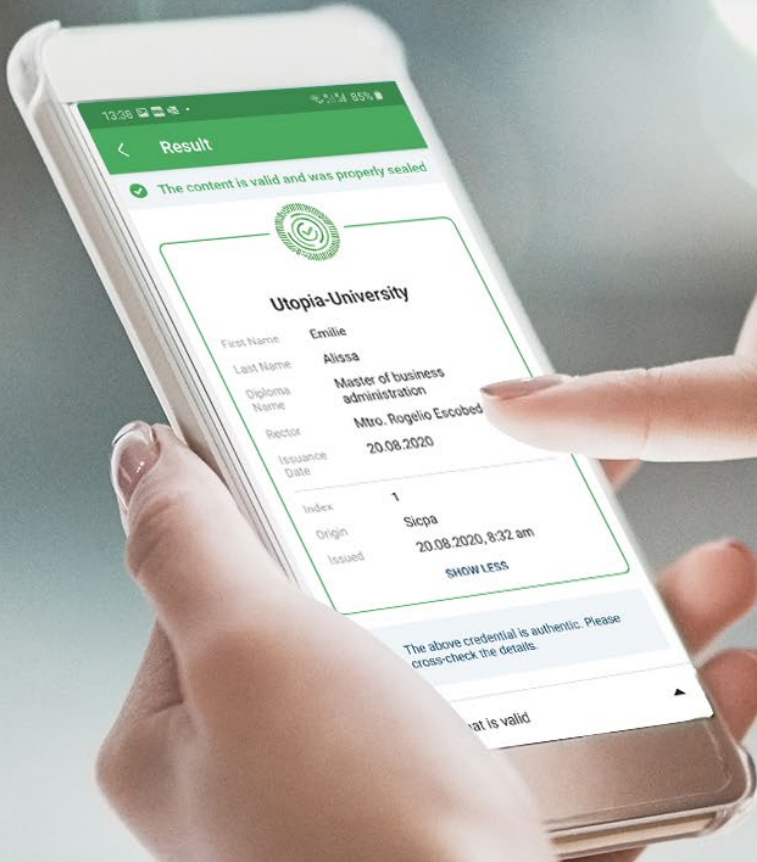
Easy to use, inclusive, universal



Enabling trust



Ultimate protection at your fingertips



BEST-IN-CLASS DOCUMENT PROTECTION AND INTEGRITY VERIFICATION

SICPA, the leading global provider of secured identification, traceability and authentication solutions and services, has created CERTUS[®], a cost-effective and easy-to-integrate solution enabling real-time digital content and printed document certification and verification. Anywhere, anytime.

It is specially designed for document issuers such as educational institutions, government bodies, notaries, local authorities and businesses to swiftly secure printed documents and digital certificates used by holders and verifiers. The solution effectively supports public and private organisations in their efforts to secure sensitive paper-based and digital content, protecting both the value of the holder's document and the issuer's reputation.

Drowning in paper?



WHO BENEFITS FROM CERTUS®



ISSUERS

The authority responsible for issuing or updating the certificate or official record can rely on CERTUS® to protect sensitive digital content and printed documents. By guaranteeing the integrity and authentication of the data at all times, anywhere, the issuer not only preserves its reputation but also reinforces trust within the holder and verifier community.

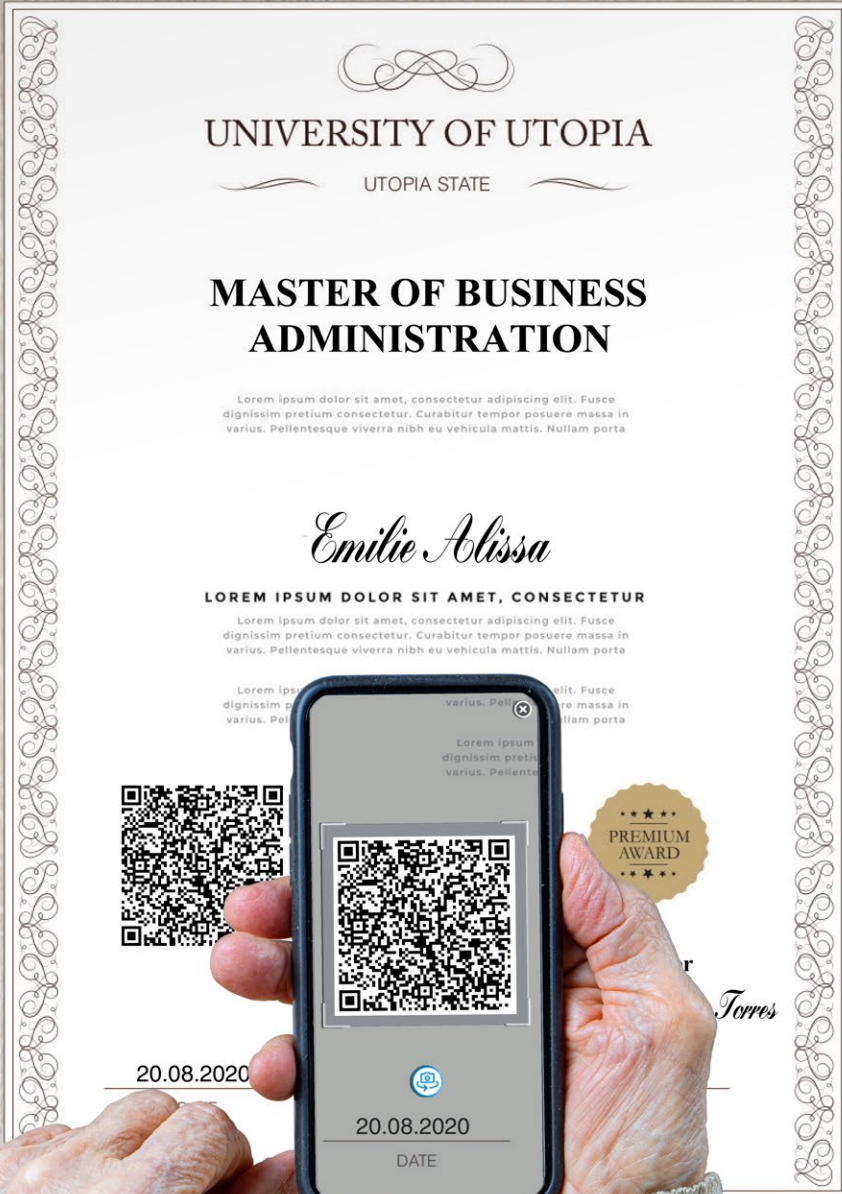
HOLDERS

Thanks to CERTUS®, holders of certified documents and data are guaranteed to be able to prove the authenticity and validity of their records and credentials at any given time. The universal applicability of CERTUS® and its freedom from third parties mean that holders can independently prove the integrity of protected information.

VERIFIERS

Verifiers worldwide, in public administration or in private organisations, benefit from the seamless service provided by CERTUS® to verify the authenticity and validity of holders' records, documents and credentials. The reliability and efficiency of the authentication and attestation process vastly reduces verification time and costs.

Document certification and verification for all



HOW IT WORKS

DOCUMENT MANAGER

Generates, activates, revokes and expires certificates

UNIVERSAL VERIFIER

Enables open and standalone verification, independent from the issuer



QR-CODE MARKING

Provides state of the art, forgery-proof security supported by a proven blockchain technology

Unforgeable QR code

The CERTUS® tamper-proof QR code protects the sensitive content directly, rather than the document itself. This makes it an ideal complementary solution to material security features for simple verification of paper and digital documents, using widely available mobile devices.

SECURED DATA IN PLAINTEXT

Issuer : Utopia University
Diploma : Master of Science
in Economics
Student : Michael Smith
Issuing date : 16.02.2020
President : Edouard Bolton
Identifier: mZ08Q=\n0GpKb4



CRYPTOGRAPHIC SIGNATURE

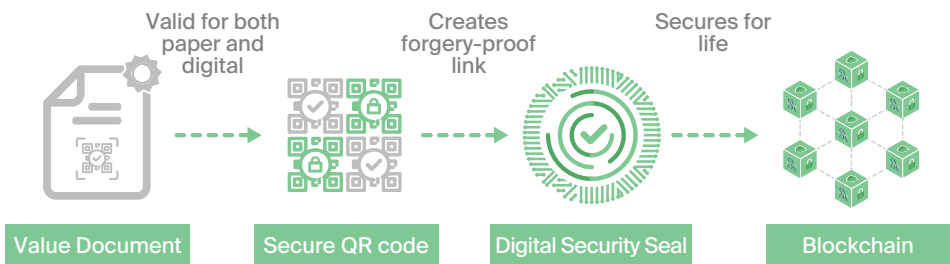
```
nBFEKqBV+HmO6Jeptymlzc  
002Pn6oK4VnCkC1H8mZ08Q=  
\n0GpKb44GsQv4VnYr8IMgflgSzqLd  
NjflGZsSnNut2Pg=\nEjP  
e/khev5GRsjT07FMbOE2RN1Ng8r+M9  
+uTzozIBV8=\nQoYpobO7XMq7kc  
PN6q1IEZWylEPkLWLhWp8YJfjks4c=
```

The QR code contains the data to be protected in plaintext and a cryptographic signature, which acts as an undisputable mathematical proof of the link between the data to be protected and its digital security seal. Anonymised or encrypted data can also be included within the QR code to preserve confidentiality.

Digital security seal

A digital security seal is used to seal the QR code and make it tamper-proof by creating a forgery proof link with the QR code's cryptographic signature. The seal is timestamped on the KSI blockchain, making the sealed document credentials immutable for life and independently verifiable without the need for a third-party guarantor.

The seal contains only metadata such as the issuer name and the date of activation. Personal and sensitive information are never stored directly, nor encrypted, in any database or on the blockchain.



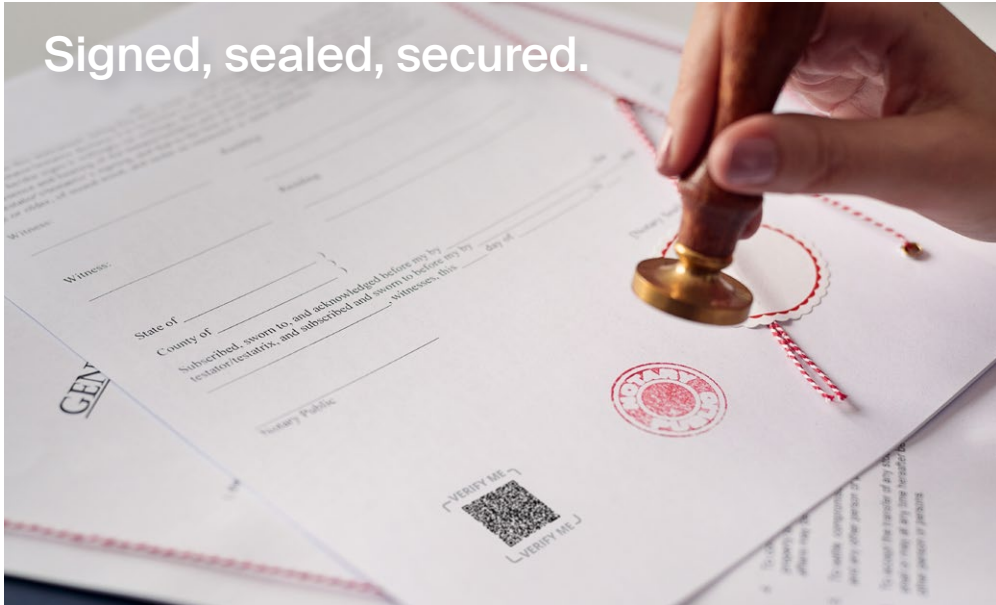
The combination of QR code, digital seal and timestamping on the blockchain makes the CERTUS® security marking virtually impossible to tamper with or forge. It makes it universally and independently verifiable for life.

Blockchain protected

Guardtime's KSI blockchain secures any digital event such as a document download, a decision, a transaction or a piece of data, as a unique fingerprint.

This service authenticates not only the time and date of the event, but also the legitimacy of the content and the author. In other words, it secures the integrity of the entire process. No sensitive data stored on the blockchain.

Signed, sealed, secured.



Bulletproof credentials

The issuance of the certificate is based on mathematical proofs that authenticate the origin and legitimacy of the following document or content credentials:

- Date and time of issuance of the document
- Name of the issuing authority
- Authenticity of the content of the credential
- Current validity of the document (active, expired, revoked)

CERTUS® sets a new benchmark in securing content and document credentials. It uniquely combines breakthrough universal digital seal technology protected by the blockchain, with a secure QR code. Securing both paper-based and digital content, the QR code marking is impossible to tamper with or forge.

Rapidly authenticate...







**...printed and
digital documents**


WHY CERTUS®


FOR ISSUERS

 **Rapid time to market, no infrastructure required**

 **Universal independent verification service**

 **Reliable, proven technology**

 **Versatile application**

 **Safeguards reputation**

Easy integration and deployment

- Online service (SaaS: Software as a Service), no infrastructure required
- Instantly operational for a wide variety of use cases
- No technical resources and expertise required
- Full automation and integration with existing IT processes can be achieved thanks to simple and open REST API
- Versatility enables solution to protect any type of data structure

Time-saving authentication

- The issuer and the protected data can be authenticated by both holders and verifiers
- Easy screening and verification of content and credentials is both time-saving and reduces costs for issuers
- Holders or verifiers can independently own the verification process without the need to contact issuers or access their systems

Universal verification

- Ever-present service ensures unlimited verification ability in time, place and form (offline/online)
- Seamless integration with existing verification systems
- Independence of verification from third parties

Strengthen reputations


- The credibility of community and individuals' assets and values is protected
- The issuer's standing is reinforced
- Trusted relationships with holders and verifiers are extended


Extensive range of applications

- Academic records
- Legal documents
- Civic certificates
- Financial reports
- Health records
- Business records

FOR HOLDERS AND VERIFIERS

 Ever-present service

 Easy to use

 Ultimate security
and confidentiality

 Inclusive

 **Seamless experience**

- Single-click authentication
- Independent verification
- Reliable and flexible
- Peace of mind for holders

 **Lifetime value**

- Lifelong validity of issued certificates
- Unlimited verification in terms of time and location
- Applicable for any verification system
- Authentication independent of any third party



Inclusive service

- Equal access to services for all
- Certification of printed and digital documents
- Holders without a digital device or computer can also make use of the solution
- Professional verifiers can use offline verification in the field in the event of low connectivity

 **Privacy protection**

- Personal and sensitive data are never stored or encrypted in any database or on the blockchain
- The QR code is self-contained and is the only place where sensitive information is stored, outside of the issuer's own system
- Compliant with European General Data Protection Regulation (GDPR)

SICPA



SICPA, ENABLING TRUST

SICPA is a recognised global expert in digital and physical security, traceability and integrity solutions. The company is a valued partner in the sphere of trust since its foundation in Switzerland in 1927, working with governments, central banks and private sector organisations.

Every day, millions of people rely on SICPA's solutions to protect the integrity of currency, preferred brands and products, personal identity documents and credentials. Through constant innovation, SICPA ensures that trust lies at the heart of its mission.

SICPA has established a global partnership with Guardtime®, the world's leading enterprise blockchain company. Guardtime®'s KSI® Blockchain has been in operation for more than ten years, securing public services for the Government of Estonia, NATO, and numerous other government entities and leading Fortune 500 companies. The KSI® Blockchain is accredited as a qualified trust service under the European Union's Electronic Identification and Trust Services (eIDAS) regulation.



Ready for easy and inclusive document certification and verification

SICPA SA

Av de Florissant 41
1008 Prilly
Switzerland

certus@sicpa.com
www.certusdoc.com
www.sicpa.com

© 2022 SICPA HOLDING SA, Switzerland
CERTUS® is a trademark owned by SICPA HOLDING SA, registered in Switzerland or otherwise protected by law.
KSI® and Guardtime® are a trademark of Guardtime registered in Switzerland and other countries or otherwise protected by law. SICPA is certified to ISO 9001:2015, ISO 14001:2015 and OHSAS 18001:2007, according to a world-wide deployment programme, in the framework of a unique Integrated Management System.