Diploma Verification

Section 1: Summary

Use Case Summary			
Use Case ID:	GOV-006	**Use Case Type**	*Vertical*
Use Case Title:	Diploma Verification	**Is uUse Case supporting SDGs**	*Yes*
		Domain:	*Government and public sector*
Status of Case	*Pilot*	**Sub-Domain**	*Education*
Contact information of person submitting/ managing the use case	*Full Name* ***Pierre-Yves Burgi*** *Job Title* Directeur SI adjoint *E-mail address:* Pierre-Yves.Burgi@unige.ch *Telephone number:* **+41 22 379 75 09** *Website:* ***https://www.unige.ch/stic/acteurs/organigramme/direction/burgi/***		
Proposing Organization	*University of Geneva, Switzerland*		
Short Description	*Pilot for verification of diplomas by Ethereum smart contract and legally recognized electronic seal. Possibility of revocation of diplomas.*		
Long description	The falsification of university certificates is a major problem. Since diplomas are often only presented as scans, forging them has become very easy. As a result, the University of Geneva is being confronted with an increasing number of verification requests. A pilot application has been developed that uses a legally regulated seal and a timestamp on a public blockchain (Ethereum) to prove the authenticity of a diploma. The document is verified by using the original PDF/A-file or a short summary of the diploma. The use of a public blockchain ensures that the diploma can be proven even in the case of the university not being able to confirm its validity anymore		
SDG in Focus (when applicable)	*SDGs in Focus are SDG 4 – education and SDG 8 – decent work.*		
Value Transfer	*No transfer of value*	**Number of Users:**	*40 (currently in the pilot), several thousand planned in the future*
Types of users	Students and everybody to whom they present their diplomas		
Stakeholders	*Students, universities, employers*		
Data:	For diplomas, only hashes are stored with no metadata added. This will only allow the verification of the originality of a document that is presented to the users. Only in the case of revocation is the information about the revocation added. However, even then, this information can only be linked to a student when somebody is in the possession of a copy of the diploma and therefore has a legitimate reason to verify its validity.		

	External recruitment systems may access the smart contract directly to verify that the documents they receive are original and have not been revoked.
Identification	Education certificates are bound to an identity and cannot be transferred. There are no anonymous certificates. The system however, needs proof that the user is already in the possession of a copy of the certificate in order to allow the verification of the certificate. Without a copy of a diploma, no personal information can be derived from the blockchain. With a copy of a diploma, only the information about the originality and the revocation status can be derived from the blockchain.
Predicted Outcomes	Less forged diplomas, less unqualified people in jobs, more trust in education, less work in verifying university certificates.

Overview of the Business Problem or Opportunity
When the recruitment process becomes digital, the proof of the authenticity of university degrees is lost. Scanned PDFs are easy to forge. The number of verification requests is rising.
Why Distributed Ledger Technology?
The solution combines a server at the University of Geneva, a regulated digital seal according to the Swiss law ZertES and a smart contract on the Ethereum blockchain. This combination was chosen for the pilot project to reach a maximum durability and to evaluate the advantages and disadvantages of the different solutions. The ultimate goal is to replace paper certificates. The advantages of DLT in this context are: • Certificates can be revoked • Certificates can be verified even when the university server is down • The blockchain-based proof does not need any maintenance by the university

Section 2: Current process

Current Solution
Until now, diplomas have only been issued on paper

Existing Flow		
Step	**User Actions**	**System Actions**
1.	Generate und print diploma	Provide data and template
2.	Apply manual seal	No automation
3.	Distribute paper diploma to students	No automation

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*Students*	Students currently scan their diplomas and use the scan in the recruitment process

Participants and their roles		
Actor	**Type/Role**	**Description**
2	*Employers*	Employers either trust the scans or manually send a verification request to the University of Geneva

Section 2: Pilot process

Pilot Solution
The pilot does not disrupt the diploma generation but is an add-on to the current process

Flow (pilot)		
Step	**User Actions**	**System Actions**
1.	Generate und print diploma	Provide data and template
2.	Apply manual seal	No automation
3.	Scan diploma	Add third page with description and generate PDF/A
4.	Confirm electronic seal	Add electronic seal
5.	Sign blockchain transaction	Calculate hashes and send them to the smart contract
6.	Send PDF/A by email and distribute physical diploma to students	Partly automated
7.	Employers receive a digital or printed copy of the diploma	
8a.	Verification of the PDF/A by employer	An employer can • verify the digital seal on the PDF/A • verify the PDF/A through the university website • calculate the hash value of the PDF/A and verify it directly against the smart contract on the Ethereum blockchain
8b.	Verification of a link (ID) by employer	The student can send a special link to the employer which acts like a key. This link will confirm the information on the diploma. The link can be deactivated
8c.	Verification of the information on the diploma	An employer can verify the information on the diploma • through the university website • by calculating the hash value of this information and verifying it directly against the smart contract on the Ethereum blockchain

Section 3: Final process

Expected Flow (Production)		
Step	**User Actions**	**System Actions**
1.	Confirm diploma to be generated	Generate PDF/A
2.	Confirm application of digital seal	Apply digital seal
3.	Sign blockchain transaction	Calculate hashes and send them to the smart contract
4.		Send signed PDF/A to students
5.	Optionally print diploma, apply physical seal and distribute it to students	Manual process
6.	Employers receive a digital or printed copy of the diploma	
7a.	Verification of the PDF/A by employer	An employer can • verify the digital seal on the PDF/A • verify the PDF/A through the university website • calculate the hash value of the PDF/A and verify it directly against the smart contract on the Ethereum blockchain
7b.	Verification of a link (ID) by employer	The student can send a special link to the employer which acts like a key. This link will confirm the information on the diploma. The link can be deactivated
7c.	Verification with the information on the diploma	An employer can verify the information on the diploma • through the website of the university • by calculating the hash value of this information and verifying it directly against the smart contract on the Ethereum blockchain

Participants and their roles		
Actor	**Type/Role**	**Description**
1	*University*	Creates the certification if student has complied with all prerequisites and sends it to the student
2	*Student*	Determines who shall be able to see and verify the diploma

Participants and their roles		
Actor	**Type/Role**	**Description**
3	*Employer, etc.*	Employer is able to verify the diploma even in the unlikely event that the university is not reachable anymore

Data and information		
Data	**Type**	**Description**
1	*Documents*	Diploma with digital seal
2	*Hashes*	Hashes of the PDF/A and of a short form of the relevant information will be written to a blockchain through a smart contract
3	*Revocation*	A revocation entry can be added through the smart contract

Security and privacy
1.Great care has been taken to provide a very high level of security and privacy. *There is a key management system for the keys that allows diploma hashes to be put or revoked to the Ethereum blockchain.* *Without already having access to a diploma, no information can be derived from the blockchain. With the diploma, no additional information is available except in case of revocation of the diploma*

Main Success Scenario + expected timeline
The pilot system works even for only one university using the system. However, universities should join forces, develop a common system or even interface with a system for self-sovereign IDs

Conditions (pre- or post-)
The final version requires the adaptation of the internal regulation of the University concerning the formal requirements of a diploma

Performance needs
With only a couple of thousands of diplomas being issued per year, the performance of Ethereum is sufficient

Legal considerations
An in-depth evaluation of GDPR was part of the project

Risks
Application of GDPR on DLT still involves some legal uncertainty.

There might be an evolving standard for university diplomas. Current diplomas might have to be migrated in the future

Special Requirements

Transaction fees need to stay manageable

External References and Miscellaneous

An in-depth description of the project can be found here:

https://erbguth.ch/slides/DiplomaPaper.pdf

Other Notes

Any assumptions, issues

Appendix 1:
Domains and subdomains for use cases categorization

Vertical:

1. Finance
    a. Financial management & accounting
    b. International & interbank payments
    c. Clearing and settlement
    d. Reduction of Fraud
    e. Financial messaging
    f. Asset lifecycles and history
    g. Trade finance
    h. Regulatory compliance & audit
    i. AML/KYC
    j. Insurance
    k. Peer-to-peer transactions
2. Healthcare
    a. Pharma
    b. Biotechnology
    c. Medicine
3. Industries
    a. Manufacturing
    b. Energy
    c. Chemical
    d. Retail
    e. Real estate
    f. IT and telco
    g. Supply chain management
    h. Transportation
    i. Agriculture
4. Government and public sector
    a. Taxes
    b. Government and non-profit transparency
    c. Legislation, compliance & regulatory oversight
    d. Voting
    e. Taxation and customs
    f. Intellectual property management
    g. Land Registries

Horizontal:

1. Identity management
2. Security management
    a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    a. Data Validation (includes provenance)