Securing physical documents with digital signatures

Christian Winter, Waldemar Berchtold and Jan Niklas Hollenbeck

Motivation

Documents have validity for certain time frame
Requirements for validity proof

- **Integrity** of the data in the document
- **Authenticity** of the issuer
- **Availability** of verification material
- **Privacy** conformity
- **Easily** validatable with wide spread equipment

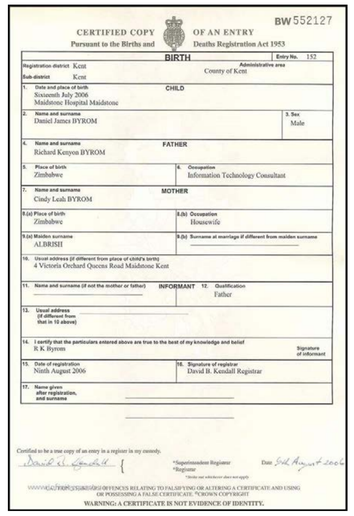
Current situation
Seal or handwritten signature is supposed to create trust

- **Integrity** of data?
- **Authenticity** of issuer?

See British birth certificate as an example

- Who is the identity behind the signature?
- Is it authorized to do so?
- Is the data, such as name, date of birth in the birth certificate integer by the signature?

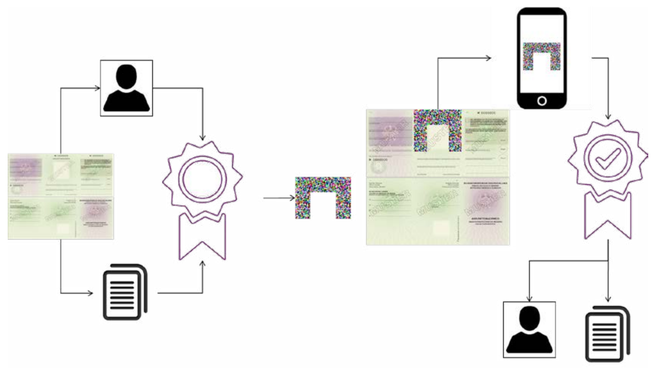
➢ **Not validatable** with seal or handwritten signature
➢ **Easy to create Counterfeits**


CERTIFIED COPY OF AN ENTRY
Pursuant to the Births and Deaths Registration Act 1953
BW 552127
BIRTH
Entry No. 152
Registration district Kent
Administrative area County of Kent
Sub-district Kent
CHILD
1. Date and place of birth: Sixteenth July 2006, Maidstone Hospital Maidstone
2. Name and surname: Daniel James BYROM
3. Sex: Male
FATHER
4. Name and surname: Richard Kenyon BYROM
5. Place of birth: Zimbabwe
6. Occupation: Information Technology Consultant
MOTHER
7. Name and surname: Cindy Leah BYROM
8.(a) Place of birth: Zimbabwe
8.(b) Occupation: Housewife
9.(a) Maiden surname: ALBRISH
9.(b) Surname at marriage if different from maiden surname
10. Usual address (if different from place of child's birth): 4 Victoria Orchard Queens Road Maidstone Kent
INFORMANT
11. Name and surname (if not the mother or father)
12. Qualification: Father
13. Usual address (if different from that in 10 above)
14. I certify that the particulars entered above are true to the best of my knowledge and belief
K K. Byrom
Signature of informant
15. Date of registration: Ninth August 2006
16. Signature of registrar: David B. Kendall Registrar
17. Name given after registration, and surname
Certified to be a true copy of an entry in a register in my custody.
Superintendent Registrar / Registrar
Date 3rd August 2006
WARNING: A CERTIFICATE IS NOT EVIDENCE OF IDENTITY.

http://opengmp.org/birth-certificate-template-uk-2/birth-certificate-template-uk-ucc1-birth-certificate-high-grade-of-birth-certificate-template-uk-download/

Proposed Approach

- Use **Digital Signature** -> satisfy requirements for validity proof
- Data and digital signature is stored in 2D Barcode and printed on document



Implementation of Approach

- Turn physical document into a digital document e.g **JSON** object
- Use well established **X.509** standard for **certificate** infrastructure
- Use **JAB Code** a polychrome 2D barcode
- Use **compression** to reduce barcode size e.g. **ZIP**

Storage Profiles

- Certificate chain up to root certificate must be available
- Revocation information is necessary to check whether a certificate has been revoked and since when
- Use Online Certificate Status Protocol (OCSP) for revocation information
- OCSP has its own certificate chain since it must be signed from its issuer as well
- Timestamp to anchor the existence of a document since a certain point in time
- Attach certificate chain of timestamp service including its OCSP information to signature
- Use Cryptographic Message Syntax Advanced Electronic Signatures (CAdES) to store mentioned information

Long-term verifiability
Examples: birth certificate, certificate of employment, training certificate

- CAdES-B-LT level (including timestamp and revocation)
- Key length for Elliptic Curve Digital Signature Algorithm (ECDSA) is chosen with 384 bits -> security level 192 bits
- Resulting JAB Code size 85x85 modules

Short-term verifiability
Examples: Medical prescription, Visa, temporary documents/certificates

- CAdES-B-B level (no timestamp, no revocation)
- Key length for Elliptic Curve Digital Signature Algorithm (ECDSA) is chosen with 224 bits -> security level 112 bits
- Resulting JAB Code size 145x145 modules

Process overview

Creation procedure

- Decide if application requires short-term or long-term profile
- Acquire a digital certificate which has an appropriate cryptographic security level. A certificate is acquired once for a certain time period
- Create JSON object containing the essential information of the document
- Create a CAdES signature over the JSON object according to the chosen profile
- Compress the CAdES signature eg with Zopfli
- Store the compressed signature in a JAB Code and print it onto the physical document

Verification procedure

- Scan the matrix code on the document and extract the data stored in the matrix code
- Decompress the data to the actual CAdES signature including the enveloped JSON object
- Validate the basic properties of the signature, ie. verify that it is a correct signature of the JSON object, and that the certificate chain correctly leads to a trusted root
- Examine the revocation status of the involved certificates depending on the scenario: In a short-term scenario, no certificate shall be revoked at verification time. In a long-term scenario, the embedded OCSP information shall be checked w.r.t. the signing time witnessed by the trusted timestamp
- Compare the content of the JSON object to the printed data. Note that this is the only non-automated step unless we automate this as well with optical character recognition (OCR)

Contact

Waldemar Berchtold
Phone: +49 6151 869-287
waldemar.berchtold@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology SIT
Rheinstraße 75 - 64295 Darmstadt