Ensuring longevity of electronically signed documents

John Erik Setsaas
2017-11-14
Disclaimer

Please note that this presentation is for information purposes only, and that Signicat has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation.

The future strategy and possible future developments by Signicat are subject to change and may be changed by Signicat at any time for any reason without notice.

This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Signicat assumes no responsibility for errors or omissions in this document.
The long term validation challenge

Verifying the signature in 5, 50 or 500 years
Seal → Authentication

Broken seal → Unauthorized access
The basement archive
• Tamper resistant
• Confidential
• Run by “TTP”

However
• Lack of «fail-over»
Cryptex with acid

Brute-force resistant storage
Agenda

• File formats and encoding
• Other challenges
• Long term signatures
• Blockchain?
• Summary
«Old» file formats

SuperCalc3(tm)
Version 2.1
IBM PC
(WITH 8087 NDP)
S/N-061668, IBM DOS
Copyright 1985
COMPUTER ASSOCIATES INTERNATIONAL, INC.

Ami Pro
Word Processing by Williams

PageMaker® by Aldus Corporation
U.S. Version 1.8
© Aldus Corporation, 1987. All rights reserved. Portions © Microsoft Corp., 1984 – 1987. All rights reserved. English Reprintation and Database © Houghton Mifflin, 1986. All rights reserved.

Visi Calc™
How did you ever do without it?
© 1979 PS Inc.
Circle 302 on Inquiry card.

EasyWriter™
a word processor from
Cap’n Software

WORDSTAR

123
Lotus

Working With DisplayWrite 4

ILBM
Encodings

For example, you may intend the text to look like this:

Author: Guðrún Guðmundsdóttir. Title: Introduction to character encoding (文字符号化入門). Copyright © 2004-2007 W3C® (MIT, ERCIM, Keio).

but it may actually display like this:


Source: www.w3.org
2017 Encodings – Printed receipt

This is what it should say

TAKK FOR HANDELEN
Åpent Man - Fre 08 - 23 Lør 09 - 22, Søn 11 - 22
Besøk oss på
www.bunnpris.no
2017 Encodings – Text message
The font-attack

I will buy your car for 9,000 EUR

Displays as

I will buy your car for 1,000 EUR

Forged font file
My access to resources on [subject] over time:

1985: Book on subject

1990: [subject].PDF

1995: [subject] web database

2000: [subject] analysis software

2005: [subject] mobile app (local university project)

2010: Site goes down, backend data not on archive.org

2015: Java frontend no longer runs

2020: Broken on new OS, not updated

Interactive [subject] CD-ROM: CD scratched; new computer has no CD drive anyway.

Library microfilm [subject] collection

It's unsettling to realize how quickly digital resources can disappear without ongoing work to maintain them.
PDF/A

“Specialized for use in the archiving and long-term preservation of electronic documents”

- ISO standard
- 100% self-contained
- All info to display is embedded
  - Text, images, fonts, color, etc
- Links to external content not allowed
  - (Except hyperlinks)
Agenda

- File formats and encoding
- *Other challenges*
- Long term signatures
- Blockchain?
- Summary
Challenge: Availability of validation data

- **Certificates**
  - Used for adding the signature
- **Revocation information**
  - Certificate validation
    - Certificate Revocation List (CRL)
    - Online Certificate Status Protocol (OCSP)
- **These services are long since gone**
Challenge: Cryptographic wear and tear

- «Holes» are found, which can be exploited
  - Forge signatures
  - Forge documents
  - Decrypt data
- Better hardware and software
  - Higher demands on the algorithms and key lengths

It’s all about math...
Challenge: When was the signature added?

Important for the order of events
• E.g. latest version of a testament
Agenda

- File formats and encoding
- Other challenges
- Long term signatures
- Blockchain?
- Summary
Preparing the signature for longevity

- Root certificate
- CA certificates
- Signing certificate
- TSA
- Trust list
- CAs
- Trust list response
- OCSP response
- Signing evidence
- PDF/A
Verifying the signature

- Everything can be verified locally
- Except the validity of the outermost root certificate
Re-sealing (periodically)

Refreshes validation data and algorithms
Agenda

• File formats and encoding
• Other challenges
• Long term signatures
• *Blockchain?*
• Summary
Re-sealing → Chain of blocks
Place a hash of the doc on the blockchain?

- **Depends on the blockchain for identification**
  - What about revocation?

- **Where to check document validity?**
  - Multiple blockchains
Place signing information on the blockchain

• **By itself, not much value**
  – It is already securely embedded in the document

• **May be sensitive?**

• **Consensus algorithm**
  – Enhance to include all certificate validation
  → Better protection against MITM attacks for OCSP and trust-list
Other issues with blockchain

• **Cryptographic wear and tear**
  – Hash algorithms broken → Refresh responsibility?

• **Will the blockchain last?**
  – For 5, 50 or 500 years
  – Transferring the trust to a new blockchain?

• **Disputes and responsibility?**

• **Time stamps?**
  – Are different blockchain timestamps synchronized?
Agenda

- File formats and encoding
- Other challenges
- Long term signatures
- Blockchain?
- **Summary**
Ensure correct visual representation → PDF/A

Simple and secure validation → Embed all info

Wear and tear → Reseal periodically

Self-contained result → Only need the root trust anchor

Blockchain → Still waiting for somebody to convince me
End of presentation

John Erik Setsaas

john.erik.setsaas@signicat.com

@jsetsaas