Chaining Electronic Seals
An eIDAS compliant framework for controlling SSCD

Przemysław Błaśkiewicz, Mirosław Kutyłowski

ACIIDS 2022

Electronic seal concept in eIDAS

electronic seal *means* ***data in electronic form****, which is attached to or logically associated with other data in electronic form to* ***ensure*** *the latters* ***origin and integrity****;*

advanced electronic seal (mutatis mutandis ← electronic signatures)

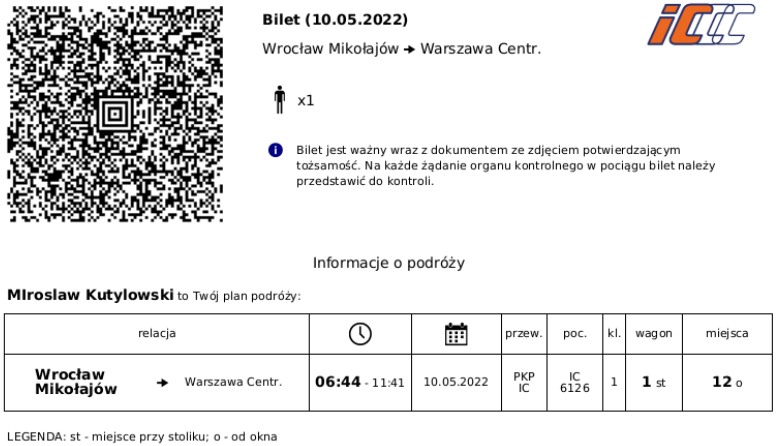
(a) *it is uniquely linked to the signatory;*
(b) *it is capable of identifying the signatory;*
(c) *it is created using electronic* ***signature creation data that the signatory can****, with a high level of confidence, use* ***under his sole control****; and*
(d) *it* ***is linked to the data*** *signed therewith in such a way that* ***any subsequent change in the data is detectable****.*

qualified electronic seal *means an advanced electronic seal, which is* ***created by a qualified electronic seal creation device****, and that is based on a qualified certificate for electronic seal;*

Application Areas

- automatically created digital documents in business and administration
  invoices and other financial documents
- **digital certificates**
- ...

Examples: tickets (cinema, train, etc.)



Bilet (10.05.2022)

Wrocław Mikołajów → Warszawa Centr.

x1

Bilet jest ważny wraz z dokumentem ze zdjęciem potwierdzającym tożsamość. Na każde żądanie organu kontrolnego w pociągu bilet należy przedstawić do kontroli.

Informacje o podróży

MIroslaw Kutylowski to Twój plan podróży:

relacja			przew.	poc.	kl.	wagon	miejsca
Wrocław Mikołajów → Warszawa Centr.	**06:44** - 11:41	10.05.2022	PKP IC	IC 6126	1	**1** st	**12** o

LEGENDA: st - miejsce przy stoliku; o - od okna

Cryptographic background

Creating digital signature

- device D holds a private key **sk**
- on input M, the device creates a signature of M:

$$s := \mathbf{sign}_{\mathbf{sk}}(M)$$

Cryptographic background

Verification of a digital signature with the public key pk

$$\textbf{Verify}(M, s, \textbf{pk}) = \textbf{valid}$$

iff

s has been created as $\textbf{sign}_{\textbf{sk}}(M)$

Cryptographic background

Key property:

it is infeasible to create a signature of M given pk and other valid signatures created with sk

Sole control

Problems

- a device creating digital signatures might be tamper-proof and resist any attempts to retrieve the private key **sk** ...
- **... but how to prevent unauthorized generation of electronic seals?**

access control is much weaker than cryptographic mechanisms,

Achilles Heel of the system!

Creative Accounting Problem

honest bookkeeping: new records only appended to the database

creative bookkeeping: old records modified, replaced, removed,...

Electronic seal alone **does not prevent creative bookkeeping**

Creative Accounting Problem

Putting all transactions in a blockchain would prevent creative bookkeeping

Do we have a cheaper solution?

- offline
- small scale and cheap
- no data leakage concerning the issuer's activity

YES!

Chain of electronic seals

Task

- given a sequence of electronic seals $S = [s_1, s_2, \ldots, s_n]$ created allegedly by a device D
- **decide whether S is the complete list of electronic seals created between s_1 and s_n**

Preventing:

- **deletions**
- **modifications**
- **insertions**

Previous work

a solution based on a hidden key in the device:

- once the key is presented to the Verifier, then the Verifier can verify a given list of seals
- ... but can also manipulate it

Przemysław Kubiak, Mirosław Kutyłowski: Supervised Usage of Signature Creation Devices. INSCRYPT 2013: 132-149

current paper:

- **hidden internal state**
- **an attacker holding signing key cannot manipulate the chain**

Solution 1

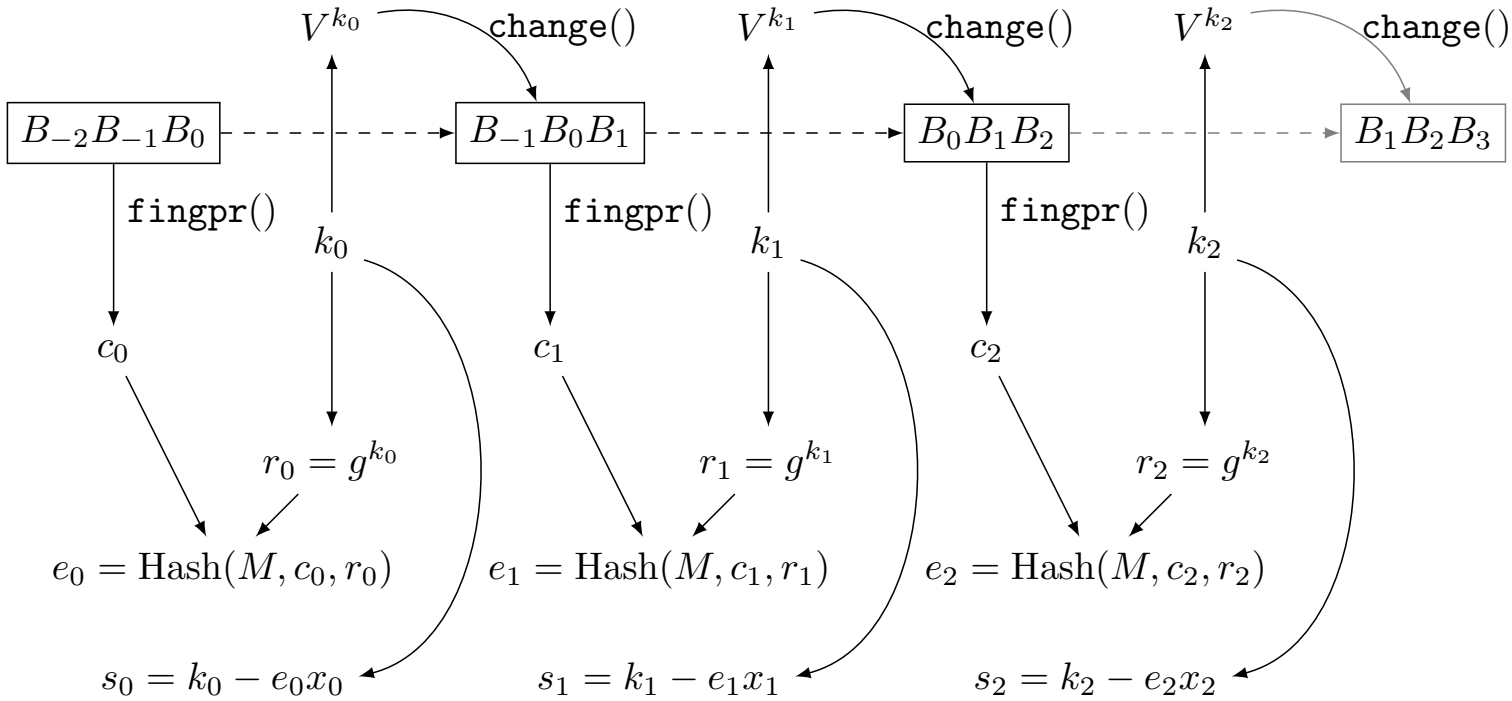
Creating chained Schnorr electronic seals

	standard steps	**additional steps**
	private key: x	state: $\mathcal{S} = (B_1, \ldots, B_t)$
1.		$c := \textbf{fingerprint}(\mathcal{S})$
2.	choose $k < q$ at random	
3.	$r := g^k$	
		$U := V^k$
4.		$\textbf{Change}(\mathcal{S}, U)$
5.	$e := \textbf{Hash}(M, c, r)$	
6.	$s := k - e \cdot x \bmod q$	
7.	output $\sigma = (e, s, c)$	

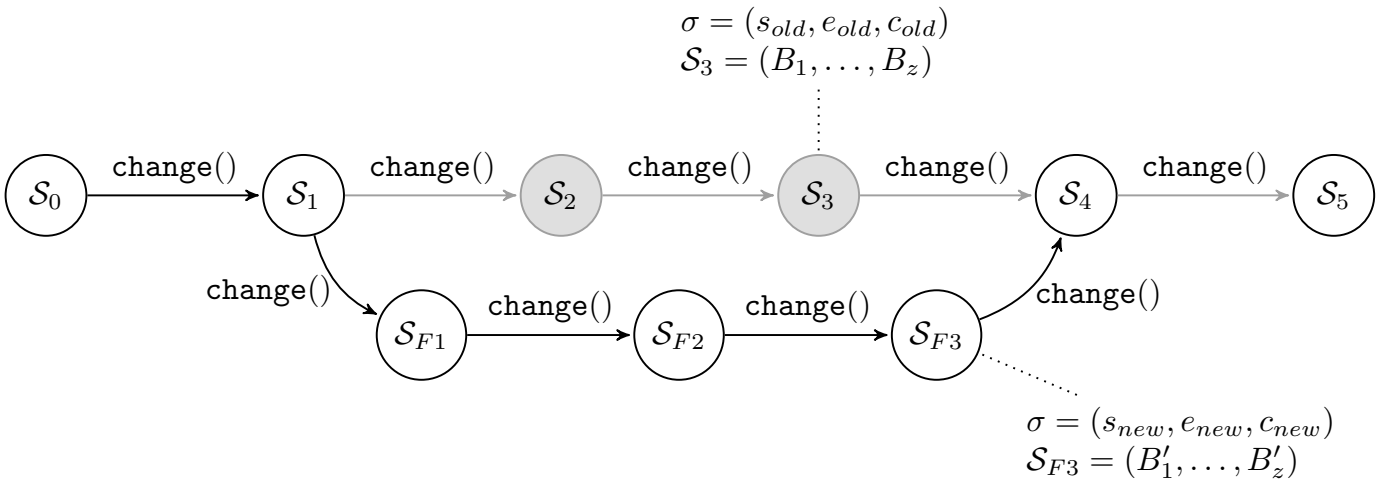
$$\textbf{Change}\big((B_1, B_2, \ldots, B_t), a\big) = \big(B_2, \ldots, B_t, \textbf{Hash}_1(a) \restriction m\big),$$

$$\textbf{fingerprint}\big((B_1, \ldots, B_t)\big) = \textbf{Hash}_2\big(B_1, \ldots, B_t\big) \restriction t\ .$$

Data flow in a chain



Substitution attempt



the problem for the attacker: the state will be affected by difference between the signatures of $\mathcal{S}_3$ and $\mathcal{S}_{F3}$ for the next z steps!

many partial collisions of the hash functions needed for the attack to succeed

in practice infeasible!

Thank you for your attention!