RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: CRYP-F01

Policy-Based Sanitizable Signatures

Kai Samelin* and Daniel Slamanig** (presented by David Pointcheval)

*TÜV Rheinland i-sec GmbH
**AIT Austrian Institute of Technology

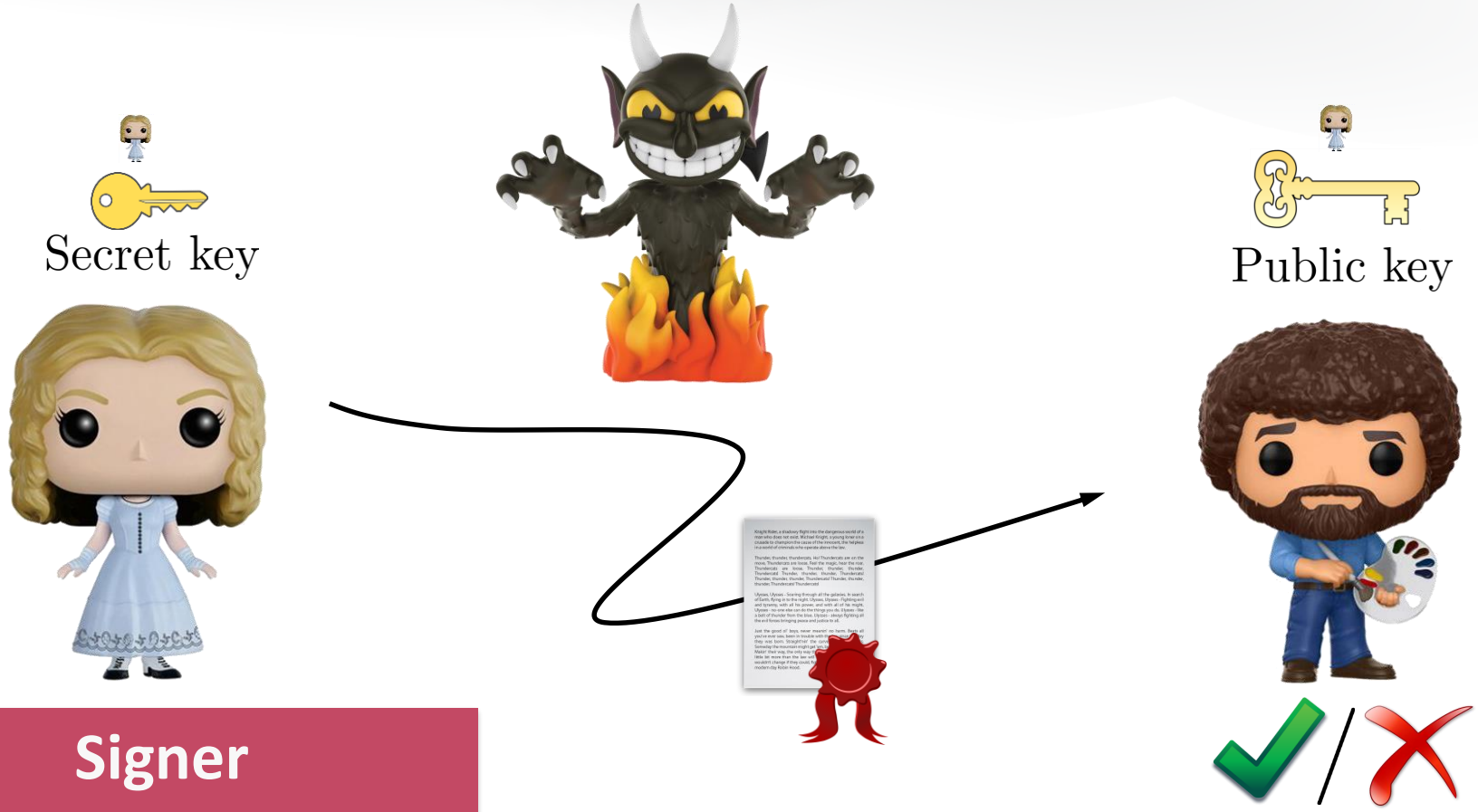
Outline

- Digital Signatures
- Sanitizable Signatures
- Policy-Based Sanitizable Signatures
- Conclusions & Take Home

RSAConference2020

Digital Signatures

Digital Signatures



Signer

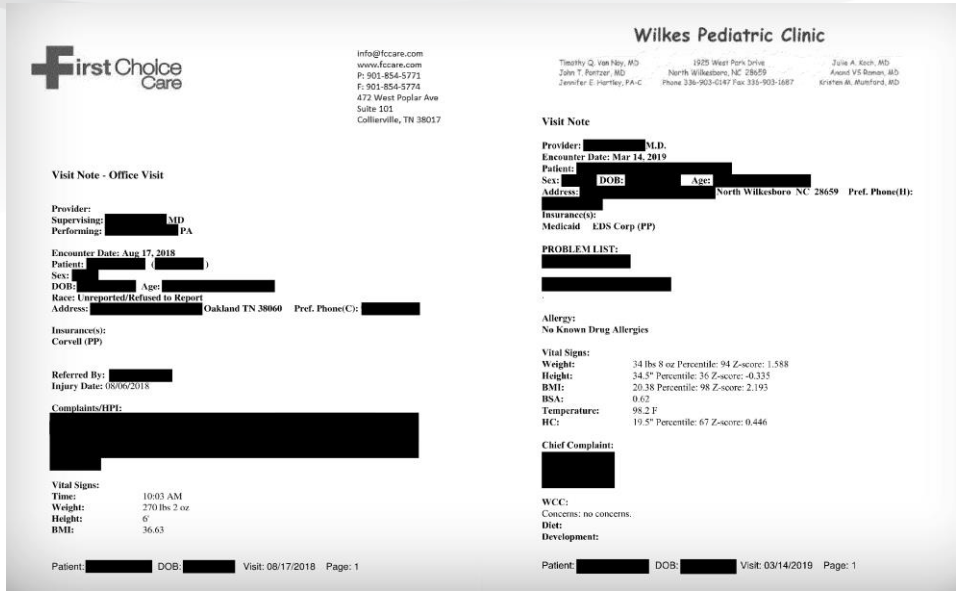
Modifications invalidate signature

Controlled Modifications of Signed Messages

- Modify signed messages without invalidating the signature?
  - But that's what we try to prevent?!
  - Can be useful **if controlled**!

- Controlled modifications
  - Signer determines ***how*** signed message can be altered
  - Think of implicitly signing all possible messages
- Control who is allowed to modify
  - Signer specifies ***entity*** allowed to perform modifications

Example: Medical Documents



First Choice Care

info@fccare.com
www.fccare.com
P: 901-854-5771
F: 901-854-5774
472 West Poplar Ave
Suite 101
Collierville, TN 38017

Visit Note - Office Visit

Provider:
Supervising: [redacted] MD
Performing: [redacted] PA

Encounter Date: Aug 17, 2018
Patient: [redacted]
Sex: [redacted]
DOB: [redacted] Age: [redacted]
Race: Unreported/Refused to Report
Address: [redacted] Oakland TN 38060 Pref. Phone(C): [redacted]

Insurance(s):
Corvell (PP)

Referred By: [redacted]
Injury Date: 08/06/2018

Complaints/HPI:
[redacted]

Vital Signs:
Time: 10:03 AM
Weight: 270 lbs 2 oz
Height: 6'
BMI: 36.63

Patient: [redacted] DOB: [redacted] Visit: 08/17/2018 Page: 1

Wilkes Pediatric Clinic

Timothy Q. Van Noy, MD
John T. Pantzer, MD
Jennifer E. Hartley, PA-C

1925 West Park Drive
North Wilkesboro, NC 28659
Phone 336-903-0147 Fax 336-903-1687

Julie A. Koch, MD
Anand VS Raman, MD
Kristen M. Mumford, MD

Visit Note

Provider: [redacted] M.D.
Encounter Date: Mar 14, 2019
Patient: [redacted]
Sex: [redacted] DOB: [redacted] Age: [redacted]
Address: [redacted] North Wilkesboro NC 28659 Pref. Phone(H): [redacted]
Insurance(s):
Medicaid EDS Corp (PP)

PROBLEM LIST:
[redacted]

Allergy:
No Known Drug Allergies

Vital Signs:
Weight: 34 lbs 8 oz Percentile: 94 Z-score: 1.588
Height: 34.5" Percentile: 36 Z-score: -0.335
BMI: 20.38 Percentile: 98 Z-score: 2.193
BSA: 0.62
Temperature: 98.2 F
HC: 19.5" Percentile: 67 Z-score: 0.446

Chief Complaint:
[redacted]

WCC:
Concerns: no concerns.
Diet:
Development:

Patient: [redacted] DOB: [redacted] Visit: 03/14/2019 Page: 1

- Tokenization for research/accounting
- Removing exact diagnosis for sick leave
- Etc.

Re-signing after the fact might not be possible (availability, etc.)

Different Types of Schemes

- Redactable Signatures
  - *Blacking out/Removal* of designated parts by *everyone*

- Sanitizable Signatures

  Replacement of **designated** parts by *designated entity*

  Designated entity (=sanitizer) has its own key pair

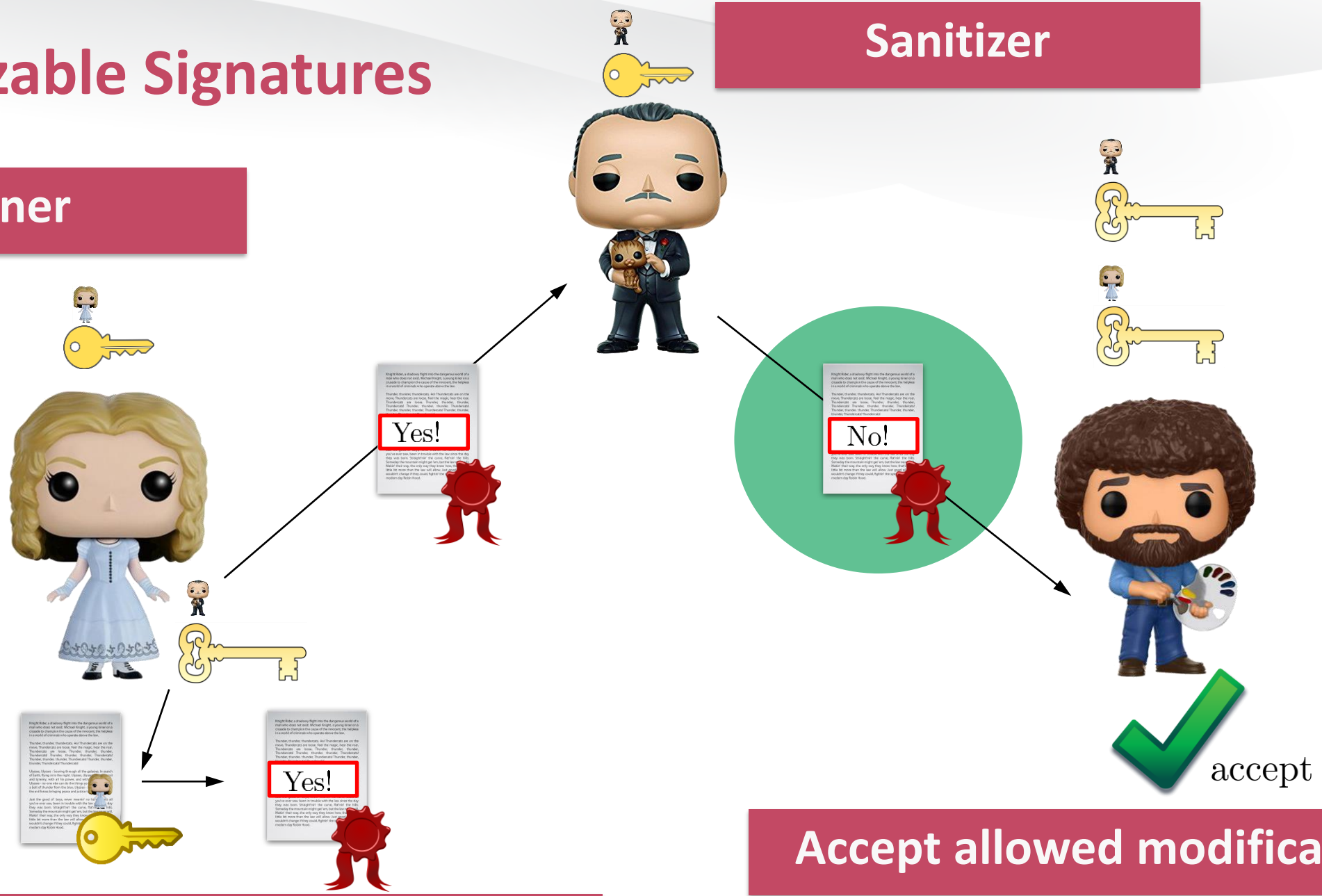
RSAConference2020

Sanitizable Signatures

Sanitizable Signatures

Signer

Sanitizer



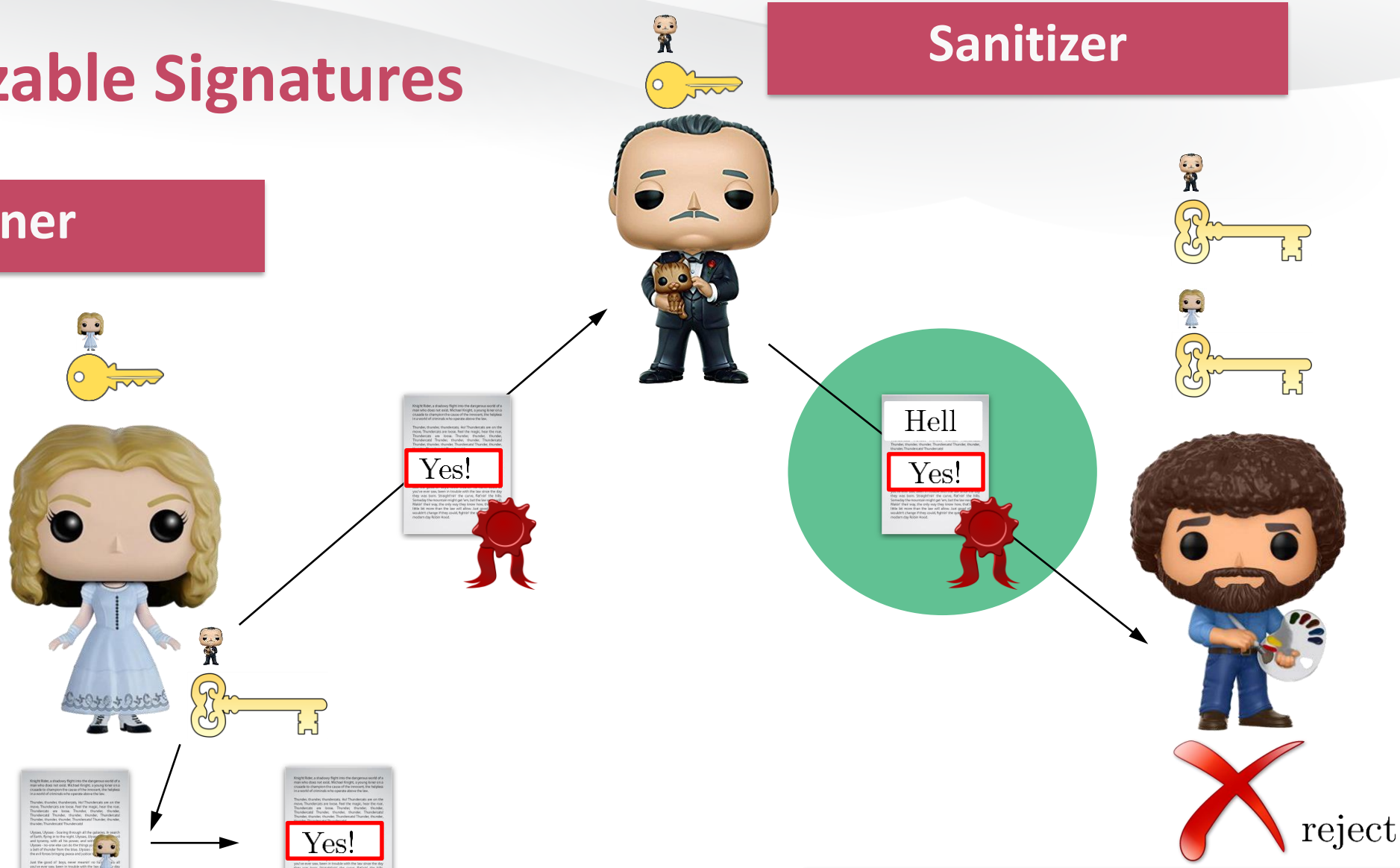
Specify modifications and sanitizer

Accept allowed modifications

Sanitizable Signatures

Signer

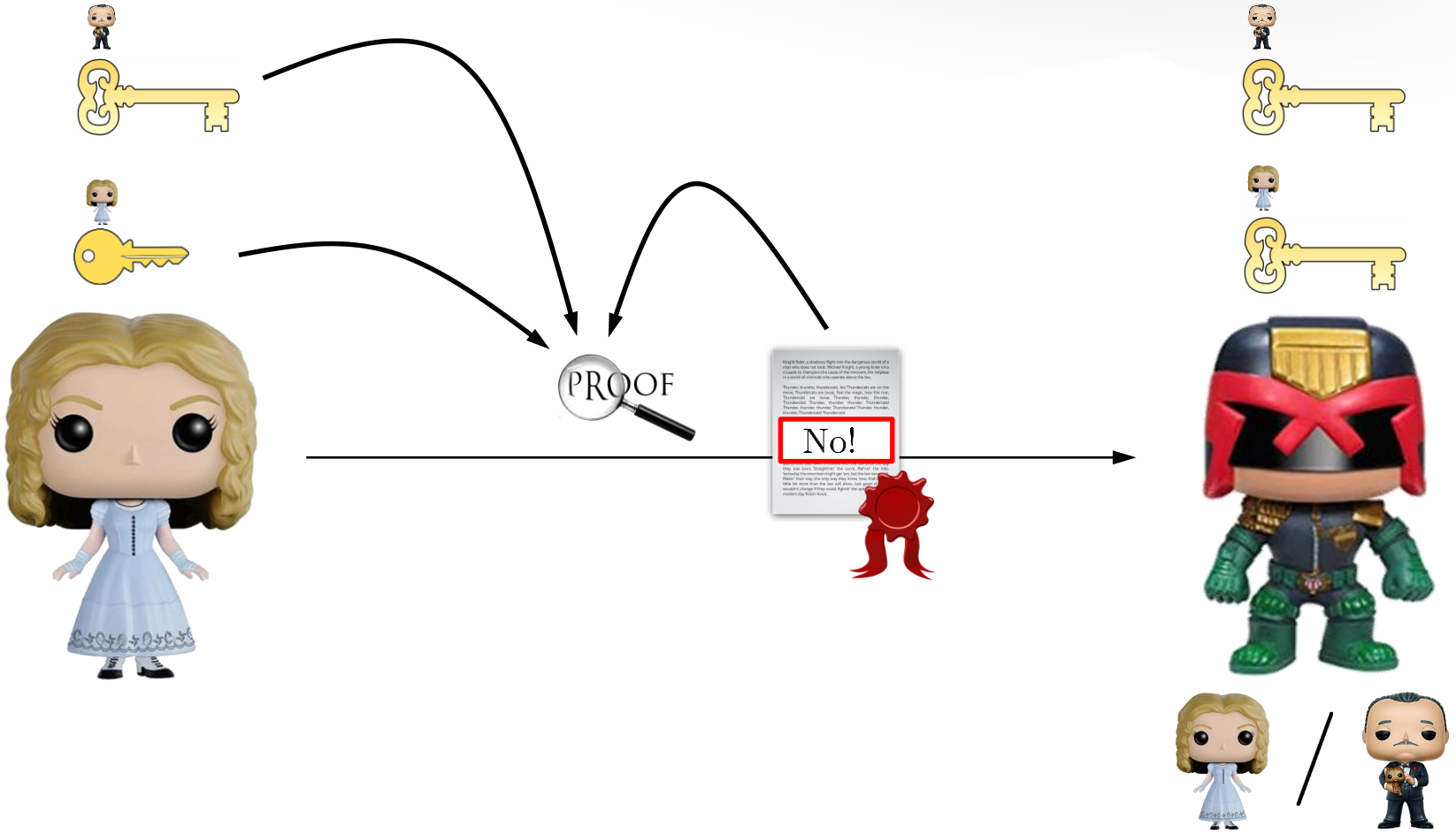
Sanitizer



Specify modifications and sanitizer

Reject disallowed modifications

Sanitizable Signatures



Generate proof that signature from signer or sanitizer

Security Properties

- Unforgeability
  - Non-sanitizers cannot come up with valid signature for non-signed message
- Immutability
  - Sanitizer cannot come up with valid signature for a message not “derivable” from signed ones
- Privacy
  - No information about sanitized parts can be learned
- Signer/Sanitizer accountability
  - Signer/sanitizer cannot blame the other party for having produced a signature
- Transparancy
  - Freshly signed and sanitized signatures are indistinguishable

Construction Idea I/II

- Originally proposed in [ACMT, ESORICS'05] and rigorous security model in [BFFLP+, PKC'09]
- Generic construction from secure signatures and *chameleon-hash functions* in [BFFLP+, PKC'09]

- Chameleon Hash [KT, NDSS'00]: Collision-resistant hash keyed with (sk, pk)
  - Hashing: $h \leftarrow \text{CHash}(\text{pk}, m; r)$
  - Collision: sk allows for any h, m' to compute r' s.t.

$$\text{CHash}(\text{pk}, m; r) = \text{CHash}(\text{pk}, m'; r')$$

Construction Idea II/II

- Simplified construction idea:
  - To sign $m = (m_1, \ldots, m_n)$
  - Use signature scheme to sign $h = (h_1, \ldots, h_n)$, where

$$h_i = \begin{cases} CHash(pk, m_i; r_i) & if\ sanitizable \\ m_i & else \end{cases}$$

  - As sanitizable signature provide signature on h; additionally include the randomness r_i of sanitizable parts

RSAConference2020

Policy-Based Sanitizable Signatures

Drawbacks of Existing Sanitizable Signatures

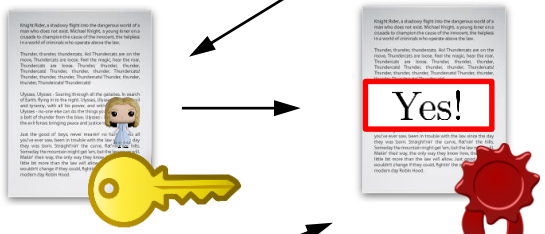
- Restricted in flexibility of specifying potential sanitizers
  - Conventional model just considers *a single sanitizer* specified *at signing time*
- Some existing works allow multiple sanitizers, but then lose accountability
  - Accountability is a central feature: sanitizers must be traceable

Achieve fine-grained sanitization control with full accountability?

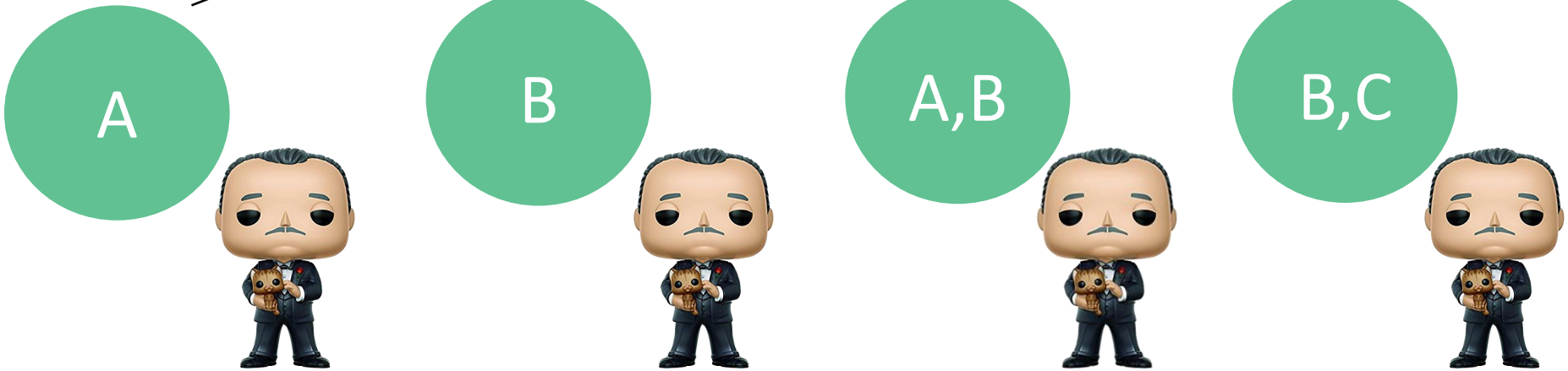
Our Vision

Signer

Specify a policy (e.g., over attributes) when signing: A AND (B OR C)



Concrete set of sanitizers not specified during singing!



Sanitizers have attributes: if attributes satisfy policy, then sanitizing works

Policy-Based Sanitizable Signatures (PB-SS)

- At signing time signer specifies an *access-policy* for sanitization and a *sanitization group*
- Sanitizers with their sanitizer key pair can *join sanitization groups dynamically*
  - Get then issued sanitization keys for attributes in the group
  - Sanitization works if sanitizer is in the group and attributes satisfy the policy
- Accountability: exact sanitizer can be identified

Achieves fine-grained sanitization control with full accountability!

Security of PB-SS

- Require same properties (but extended) as for sanitizable signatures **plus**
- Pseudonymity
  - Signature does not leak which party is accountable
- Proof-Soundness
  - Impossible to generate a proof for an adverserially chosen signature/message pair that points to different entities
- Traceability
  - Impossible to generate a verifying signature such that an honest signer cannot identify the accountable party

We also further strengthen (existing) notions whenever possible

Construction Idea: PB-SS

- Follows basically the idea outlined for sanitizable signatures
- Instead of using a chameleon hash we use a strengthened version of a policy-based chameleon hash [DSSS, NDSS'19]
  - Hash is computed with respect to a policy
  - Collisions can be found when policy is satisfied
  - Can be constructed from chameleon hashes with ephemeral trapdoors [CDKPSS, PKC'17] and CCA secure ciphertext-policy attribute-based encryption (CP-ABE) [BSW, Oakland'07]
- Achieving accountability requires some additional technicalities
  - Use of a non-interactive zero-knowledge proof (NIZK) for an OR-language

Potential Application of PB-SS

- Applicable to all existing applications
- A new application can be *redactable blockchains*
  - Introduced by [AMVA, EuroS&P'17]
  - [DSSS, NDSS'19] introduce the use of PBCH to hash transactions in blockchains
    - Update/rewrite transactions by computing collisions in the PBCH
    - Fine-grained approach by using policies
  - Use of PB-SS instead of PBCH to get additional properties such as accountability

RSAConference2020

Conclusions and Take Home

Conclusions & Take Home

- Sanitizable signatures are a tool to realize controlled modifications of signed messages
- Existing schemes are very limited in their expressiveness
- We introduce the notion of policy-based sanitizable signatures
  - Fine-grained sanitization control via policies
- We present a strong security model and a provable secure practical construction