INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES

CISPA
Center for IT-Security, Privacy and Accountability

Legal requirements for cryptographic security: Necessity, annoyance, or both?

Christoph Sorge

juris Professorship of Legal Informatics
Saarland University

My institutions @ Saarland University

Institute of Law and Informatics

- Interdisciplinary legal and technical research
- Part of Saarland University‘s Law School
- Five professors, including one computer scientist

www.rechtsinformatik.saarland

Center for IT Security, Privacy and Accountability (CISPA)

- About 200 IT security researchers
- Federal funding as one out of three IT security research centres
- Soon to become an independent research centre with increased federal funding – 500+ researchers

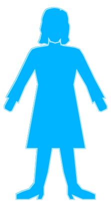
www.cispa.saarland

Cryptography is more than encryption

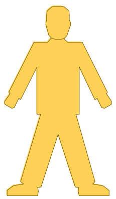
(Some) protection goals in cryptography

- Confidentiality:
  Alice sends Bob a message. No one other than Alice and Bob should be able to read the message

Encryption



Alice



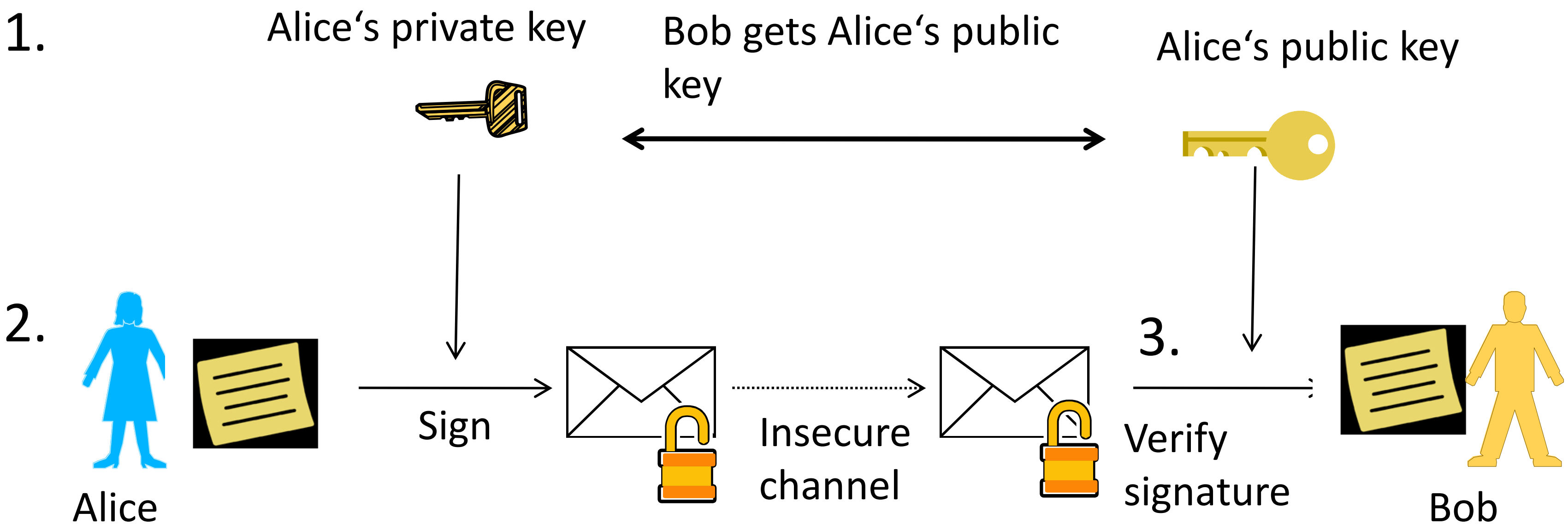
Bob

- Authenticity:
  Alice sends Bob a message. Bob shall be able to check whether the message is actually from Alice.
- Integrity:
  Alice sends Bob a message. Bob shall be able to check whether the message was tampered with on its way to him.
- Non-repudiation:
  Alice sends Bob a message. Bob shall be able to prove to a third party that Alice sent that message.

Digital Signature

Digital signatures

- Digital signatures use asymmetric cryptography: Different keys for sender and receiver



Fails if message was
- not signed with Alice‘s private key
- or changed afterwards

Application of digital signatures

- Obvious application of a cryptographic digital signature
  - Confirm authenticity and integrity of documents by signing them
- Less obvious applications
  - Secure the exchange of cryptographic keys for secure communication
  - Confirm transactions in Bitcoin and other Blockchain-based systems
  - …

Legal aspects of signatures

- Concept of signing documents: Much older than asymmetric cryptography
- Focus on natural persons (but: similar concepts for legal entities)

- Goals:
  - Ensure authenticity of documents
  - Symbolize that the signer takes responsibility for a document
  - Provide evidence that the signer wanted to make a certain declaration
  - Warn the signer that his action has legal relevance
  - Mark the end of a document

The connection

- Similar goals of signatures (in law) and cryptographic digital signatures
→ use cryptographic signatures in (legal) transactions

- Legal consequences to the use of signatures
→ requirements should also be determined by law

Regulation approaches

- ESIGN Act, USA:
  The term `electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record

→ No cryptography necessary

→ Limited value of electronic signatures as evidence

Regulation approaches

- eIDAS regulation, European Union:
  'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- *'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;*
- *'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures*

→ Three levels of signatures with different requirements (and consequences)

Issues

- Level of detail of regulation
  - “use of state-of-the-art algorithms”
  - or “use of the RSA algorithm with key length of 2048 bits or more and combined with the SHA-256 function…

    as implemented in software XYZ, version 1.3”?

- Problem of technical/mathematical progress

Technical/mathematical progress

- Cryptography is thousands of years old
- Mathematical understanding of cryptography is new (few decades old), asymmetric cryptography about 40 years old
- 1977: First algorithm for asymmetric encryption and signatures published by Rivest, Shamir, Adleman
  - Independently invented by GCHQ employee Cocks in 1973, but kept secret till 1997
- Still in common use for encryption and for signatures
- Security based on hardness of finding the prime factors of large numbers

Technical/mathematical progress

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541

- Shown here: 129 digit number, used in 1977 as RSA key for a "challenge"
  - Finding the two prime factors allows decryption of an encrypted sentence (equal difficulty: Forging of signatures)
  - Conservative estimate by Ron Rivest, 1977: Time for finding the prime factors > 40 quadrillion years (quadrillion: 10^{15})
  - Challenge solved in 1994

- Solution: **The Magic Words are Squeamish Ossifrage**
  - Bird shown to the right

Source: Richard Bartz, München, via Wikipedia

Technical/mathematical progress

How to deal with technical and mathematical progress?

- Impossible for legislation to keep up with technical developments

→Refer to state of the art:

- Vaguely ("use of state-of-the-art systems") or implicitly ("data that the signatory can, with a high level of confidence, use under his sole control")
- By naming specific standards (e.g. German approach under current signature legislation: federal agency publishes an "algorithm catalogue" on a regular basis)

→ Shifting responsibility to experts in different ways

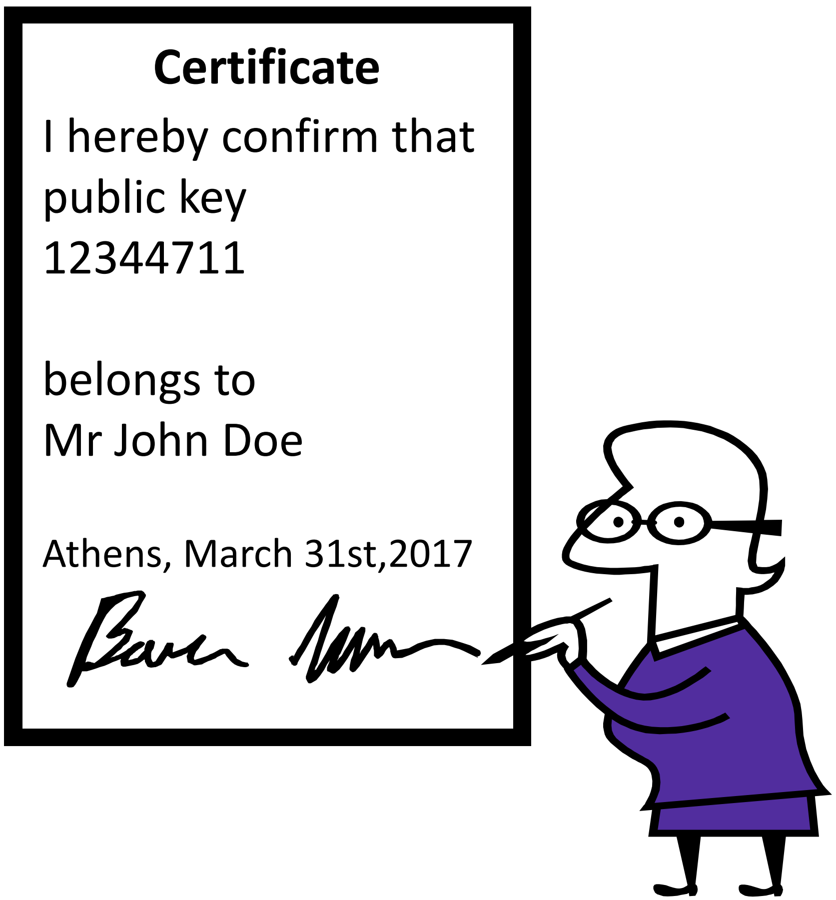
Beyond algorithms

- Cryptography is about algorithms and data
  - What can be done with private and public keys?
  - How can security be achieved against attackers who do not have certain keys?

- Law is about real-world issues
  - Who was the person that signed?
  - How does the identity have to be verified?
  - How well must access to private keys be protected?

Certificates

- From keys to identities: Certificates



- Documents confirming that a specific public key belongs to a specific person
- Signed by a trusted authority (certification authority)

→ Only the public keys of the authorities have to be known

Example

eIDAS regulation, Article 26

An advanced electronic signature shall meet the following requirements:

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 [=private key] 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.

Legal vs. technical definitions

- *[The advanced electronic signature] is uniquely linked to the signatory;*

→Not generally a requirement in technical definitions of signatures

→Implicit assumption in cryptographic signature definitions: Key pairs are uniquely linked to the signatory (not the signatures created using the keys)

→Attack: Generate second key pair that creates the same signature for a given document

→Legal definition is stricter

Legal vs. technical definitions

- eIDAS regulation, Article 3 (12)
  'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

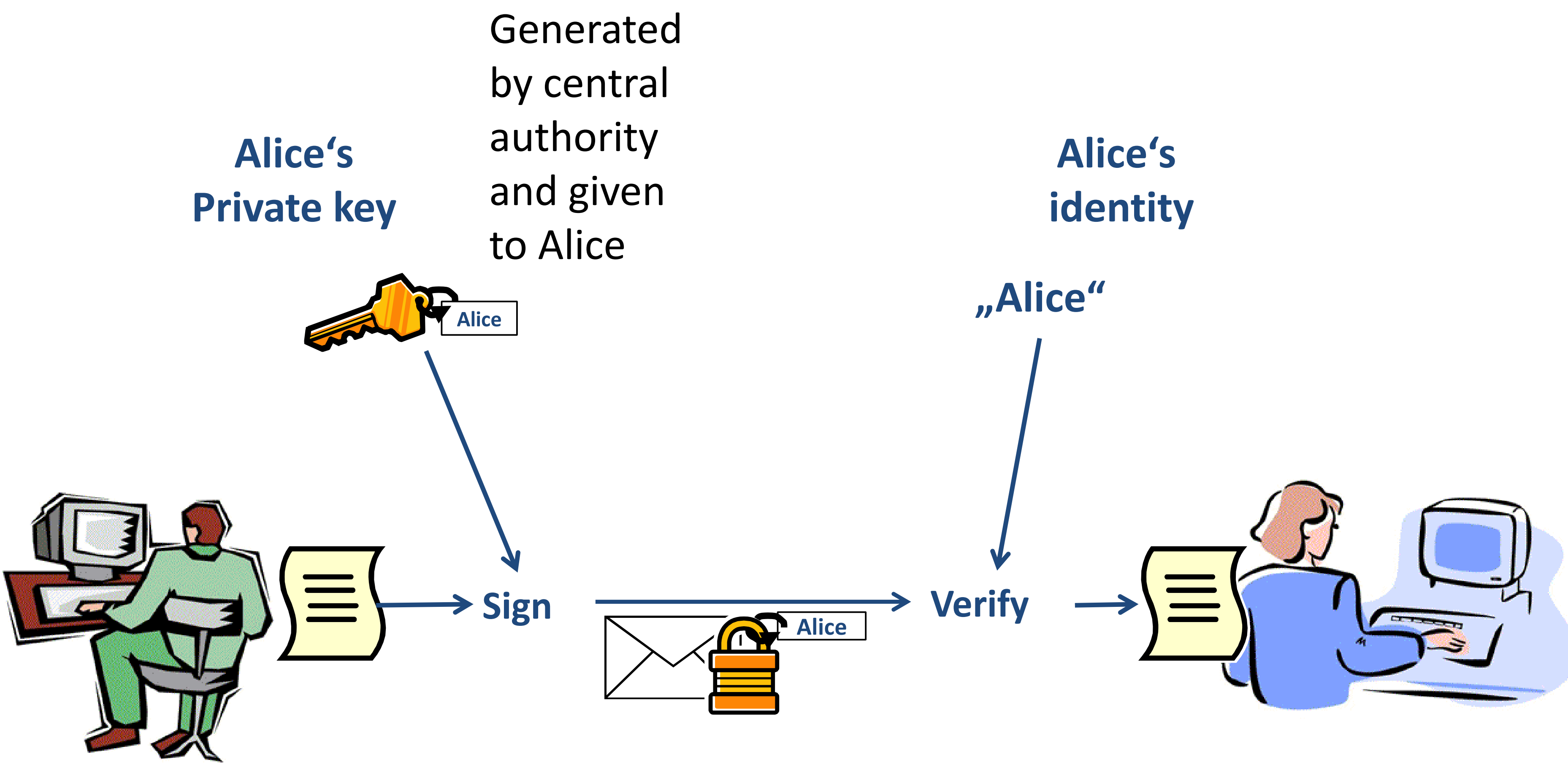
→ Requirements for secure storage of the private key and for certificate issuing

Legal vs. technical definitions

- Goal of the signature legislation: to be "technology neutral"
- Implementation of the signature legislation: Trying to match classical public-key cryptography very closely, but exchanging some terms
- Is there something else?

Cryptography

- Identity-based Cryptography (here: signing, concept also works with encryption)



Legal vs. technical definitions

Issues of “sole control”

- Private key must be generated by someone other than the signatory (private key generator)

  → is it under the signatory’s sole control?
- Private key generator can impersonate anyone

But:

- eIDAS regulation allows remote signatures (signature generation handled by a third party)
- Generation of private keys by traditional certification authorities is also allowed (they may not keep copies)
- Traditional certification authorities can impersonate anyone

→ relatively minor differences, sole control no longer an issue

Legal vs. technical definitions

- Issues of “certificates”

eIDAS Article 3 (13): Certificate = “*an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person*”

- In identity-based cryptography: Attestation is only generated by the signatory at the time of signing
- Certification authorities for qualified certificates must maintain a certificate database

→ not possible for identity-based signatures

→ No qualified signatures with identity-based cryptography

Technology neutral legislation?

Beyond signatures

Other intersections between cryptography and law

- Data protection legislation: Should encrypted data be considered as personal data?
- Critical infrastructure protection: Requirements for the use of cryptography?

- Common misunderstanding: Cryptography seen as the core problem of information security (e.g. German telecommunications act requires use of “a particularly secure encryption scheme”)

Conclusion

- Regulating electronic signatures makes sense
- Existing signature legislation is not technology neutral (is this a problem?)
- Core issue: Limited perception of foundational research in the political domain
  - Not just signatures, but privacy-related cryptographic schemes (anonymous credentials etc.) as well
- How much responsibility can/should be shifted towards cryptographers?
- How can communication between the communities be improved?

Thanks for your attention

Contact:

www.legalinf.de

christoph.sorge@uni-saarland.de