Biometric Authentication

https://iuk.one/1033-1009

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock,Germany
clemens.cap@uni-rostock.de

Version 1

Overview

1. Biometric Methods

Which biometric methods for authentication are there?

Hand Geometry (1)

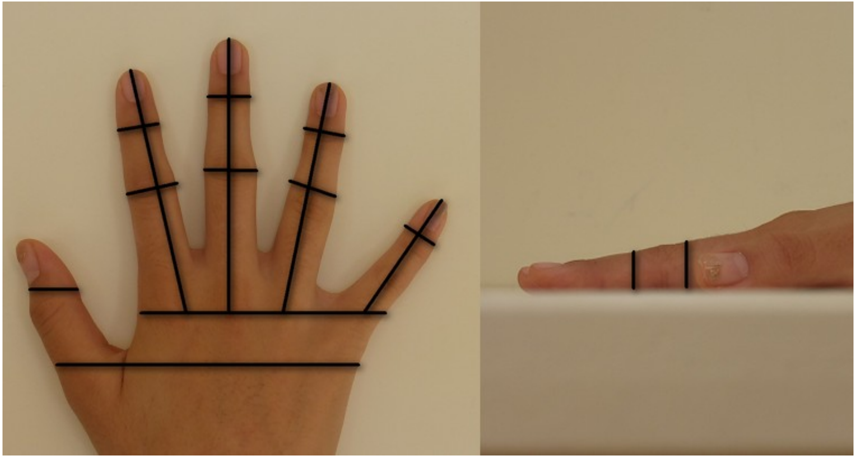

Fig. 1: Using hand geometry for biometric authentication © Rights see appendix.

Hand Geometry (2)

Evaluation:

- Convenient and fast rendering of signal.
- Comparison algorithms relatively easy.
- Error rate of 0.1% is bad.
- Not considered secure enough.

Fig. 2: Device for reading hand geometry. © Rights see appendix.

Fingerprint (1)

Fig. 3: Details of a fingerprint © Rights see appendix.

Fingerprint (2)

Fig. 4: Whorl, arch and loop are three basic patterns of fingerprints © Rights see appendix.

Fingerprint (3)

Evaluation:

- Optical, capacitive, thermal or ultrasound derivation of fingerprint structure.
- Preprocessing and detection of characteristic features ("minutiae").
- Storing and mapping only the minutiae structures prevents easy duplication.
- Fast and convenient.
- Error rate of 0.01% - 0.00001%, highly dependent on sensor and method.

Face (1)

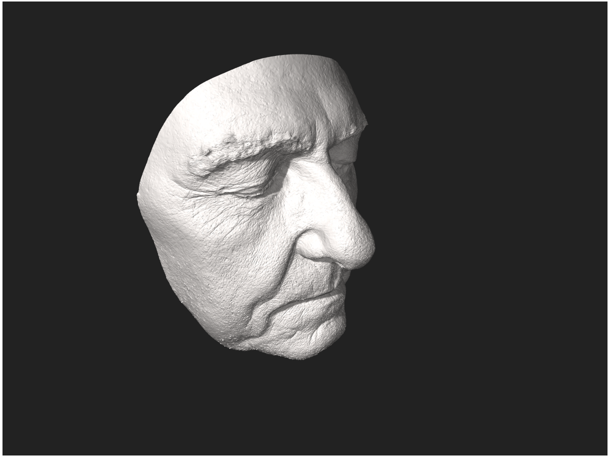

Fig. 5: 3D facial data for use in biometric authentication © Rights see appendix.

Face (2)

Overview:

- 2D or 3D Camera image
- Complex matching algorithms.
- Looks like it becomes the method of the future.

Specific Problems:

- Facial changes: Sunglasses, beard, makeup. Require advanced learning algos.
- Faking with facial masks.
- Signal rendering when wearing (Corona) masks.
- Twins.

Evaluation:

- Rendering of signal outside of control of the user.
- Access to the original signal cannot be kept under control.
- Improvals: Require open eyes or eyes looking at screen.

Iris (1)

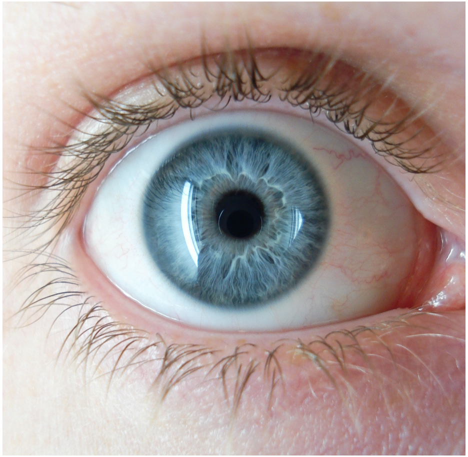

Fig. 6: Iris structure © Rights see appendix.

Iris (2)

Evaluation:

- Well protected body part (no wear as in fingerprints).
- Resistant against tampering, damage, wear and change.
- Signal remains stable for over 30 years.
- Commercial sensors easily tricked by images.
- Live-detection using pupillary reflexes is possible.
- Currently becoming more and more common.
- Can develop into privacy issue: Very reliable and can be made to work at distance.

Retina (1)

Fig. 7: Retina blood vessel structure © Rights see appendix.

Retina (2)

Evaluation:

- Very secure method.
- No two people have the same retina structure.
- Sensors expensive.
- Scanning procedure considered invasive and cumbersome.
- Eye diseases can affect rendering process and accurary.

Voice

Two forms:

- Active voice authentication: Using a particular passphrase.
- Passive voice authentication: Continuous authentication in parallel to a voice communication.

Evaluation:

- Not very reliable.
- Danger of faking by audio recordings.

DNA

Evaluation:

- Highly reliable.
- Theoretical risk of coincidental match: 1 in 100.000.000.000
- Practical risk of coincidental match: 1 in 1.000 (due to twins!)
- Useful for forensic examination.
- Problematic for IT authentication (time, costs, sample collection).

Keystroke Dynamics

Elements of the signal:

- Duration a key is pressed.
- Time between releasing one key and pressing another.
- Variants: Using left or right shift-key.

Looks attractive:

- No particular device needed for picking up signal.
- Continuous authentication of a PC user throughout a session.
- Highly acceptable.
- Difficult to circumvent.

Problem:

- Error rate is (too) high (1-2%) and varies throughout the day.
- Allows user tracking

Offered by http://www.typingdna.com in a SaaS setting.

Further Methods

Body Geometry

- Veins in hands or arms — Company Whitepaper
- Structure of ear — Paper

Behavioral Aspects

- Signature — Paper
- Gait — Paper
- Smell — Paper

2. Quantitative Evaluation

How do we evaluate the quality
of a biometric matching algorithm?

Which quantitative measures are known?

Confusion Matrix

Situation:

- A test predicts a condition.
- This produces a confusion matrix.

	Condition present	Condition not present
Condition predicted	True Positive	False Positive
Condition not predicted	False Negative	True Negative

Tab. 1: Confusion Matrix

Goal:

- Ideally: False Negatives and False Positives should both be small.
- Practically: There always is a trade-off.
- Compare: A "test" predicting condition always – has no false negatives.
- Compare: A "test" predicting condition never – has no false positives.

Medical Tests: Sensitivity and Specify

Medical tests work with sensitivity and specifity.

$$\textbf{Sensitivity} = \frac{\text{TP}}{\text{Condition Present}} = \frac{\text{TP}}{\text{TP+FN}}$$

$$\textbf{Specifity} = \frac{\text{TN}}{\text{Condition Not Present}} = \frac{\text{TN}}{\text{TN+FP}}$$

High sensitivity: The prediction does not miss the condition when it is present but possibly does so at the costs of producing many false positives.

High specifity: The prediction does not wrongly indicate the condition but possibly at the costs of missing some cases where the condition is present.

Task: Covid Test

According to studies, a SARS-CoV2 test by Roche showed a sensitivity of 90.6% and a specifity of 98.6%. See: Roche Press Release

Assume:

- In one week, all the 100.000 inhabitants of Fantasy Town are tested.
- 30 persons are Covid positive (condition present; ground truth).

Tasks: Determine all values of the confusion matrix and:

- How many persons are false positive (incorrectly testing positive)?
- How many infected persons are not detected?
- What is the incidence value determined for Fantasy Town as basis of this test?
- What is the minimal specifity a test must have, that Fantasy Town has an incidence value of 50 or less?

Disclaimer: I am not a medical doctor. I am not rendering medical advice. I am not an expert in epidemiologie. The task given here is only for illustrative purposes and no medical or other conclusions should be drawn from it. The given data are assumed or published by the manufacturer and are used without further plausibility or background checks. Tests used for incidence values are different from the kind of tests whose data are used here.

Document Retrieval: Precision and Recall

Document retrieval works with precision and recall.

$$\textbf{Precision} = \frac{\text{TP}}{\text{Condition Predicted}} = \frac{\text{TP}}{\text{TP+FP}} = \frac{\text{relevant and retrieved}}{\text{retrieved documents}}$$

$$\textbf{Recall} = \frac{\text{TP}}{\text{Condition Present}} = \frac{\text{TP}}{\text{TP+FN}} = \frac{\text{relevant and retrieved}}{\text{relevant documents}}$$

Precision: Fraction of retrieved documents that were relevant.

Recall: Fraction of relevant documents that were retrieved.

Biometrics: False Match and False Non-Match Rate

Biometrics works with False Match Rate and False Non-Match Rate.

$$\textbf{False Match Rate (FMR)} = \frac{\text{FP}}{\text{FP+TN}} = \frac{\text{Falsely Admitted}}{\text{All Admitted}}$$

$$\textbf{False Non-Match Rate (FNMR)} = \frac{\text{FN}}{\text{TP+FN}} = \frac{\text{Falsely Rejected}}{\text{All Rejected}}$$

False Match Rate (FMR): Proportion of impostors that are falsely admitted among all admitted persons.

False Non Match Rate (FNMR): Proportion of genuine subjects that are falsely rejected among all rejected.

Task: Airport Biometrics

Background:

- Chose two different biometric methods suitable for airport indentification.
- Research in the Web for their FMR and FNMR values.
- Assume the methods are used at Frankfurt airport (use pre Corona numbers of passengers).
- Assume no impostors want to enter the country ot thr planes.

Determine the number of persons who, on an average day, will be falsely accused by the biometric check system of using fake identity.

Criterion Curve

- Test produces a value (eg: closeness of signal to template).
- User choses limit which distinguishes match from non-match.
- Choice produces the two tradeoff values.

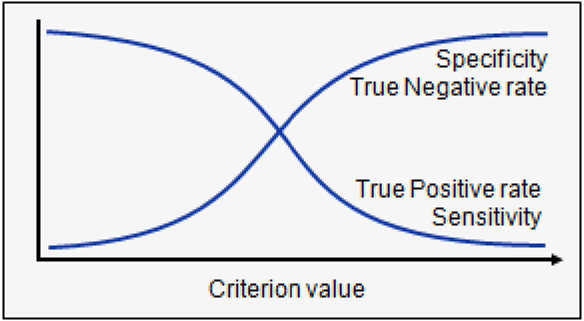

Fig. 8: Choice of criterion limit value affects the two tradeoff values © Rights see appendix.

Receiver Operating Curve (ROC)

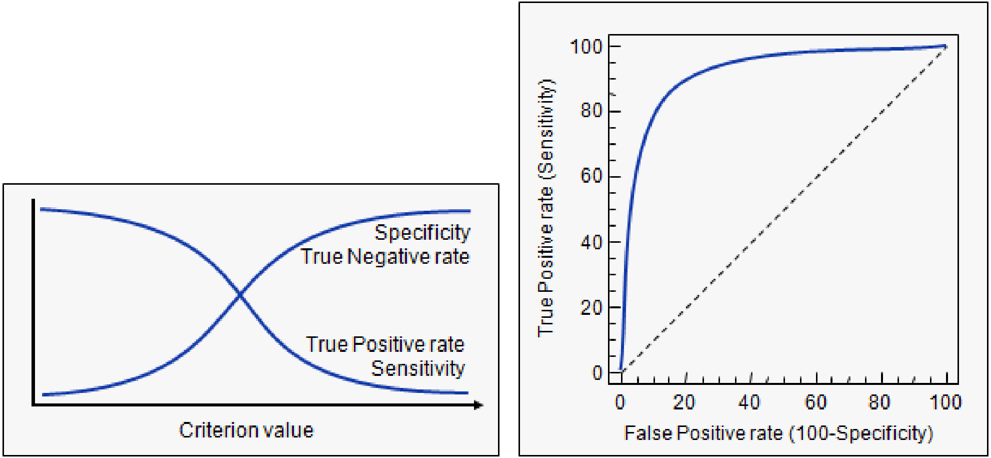

Fig. 9: The receiver operating curve (right) illustrates the dilemma contained in the criterion curve (left).

Area under the Curve

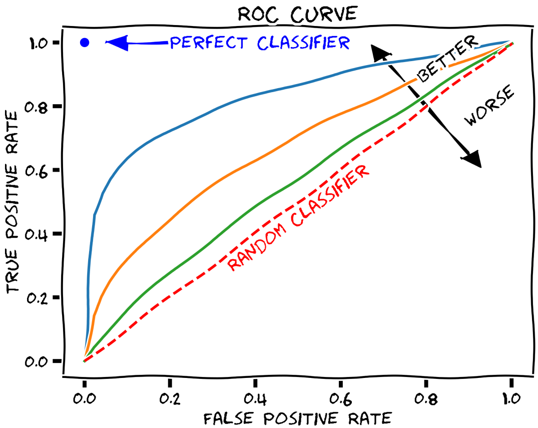

Fig. 10: The **area under the curve** is a good global measure for the quality of a detection algorithm. For pure guessing we get 0.5, for the perfect classifier we get 1. The closer the value to 1, the better.

Deciding on the Operating Point

Question: How do we chose the operating point?

Leads to: Which type of error do we perceive as worse?

Example:

- Is it worse to have a murderer go free?
- Or is it worse to imprison an innocent person?

Example:

- Is it worse to admit a non-entitled person to your bank account?
- Or is it worse to lock you out from your bank account?

Equal Error Rate

Biometry often choses **point of equal error rate:** FMR = FNMR.

Question: How good is the method as such at this point?

Answer: At the particular operating point, look at the accuracy:

$$\textbf{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} = \frac{\text{True Predictions}}{\text{All Predictions}}$$

Typical accuracies:

- 1 in 100 considered basic
- 1 in 10.000 considered medium
- 1 in 1.000.000 considered good
- Hard to get independent studies: Evaluation needs mass study & money.
- Trust into manufacturer studies? Be aware of conflict of interest.

Failure to Capture

Failure to Capture

In how many cases does capturing a live signal fail?

Problem for mass-use and for convenience of end-user.

Examples for fingerprint biometrics:

- Dirt, paint or glue on finger.
- Cut on finger.
- Skin disease.

Failure to Enroll

Failure to Enroll

How often does the enrollment process fail
after repetitive capture under supervision of a trained biometric expert?

Note: Different from Failure To Capture

Examples for fingerprint biometrics:

- Forrest worker with damaged fingerprints.
- Disabled people.
- Very young or very old people.
- People with intentionally low cooperation on enrollment.

Evaluation:

- In UK study for fingerprints: 0.7 – 3%
- Thus: Need to ensure that a replacement method is available!

Low Cooperation

Fig. 11: Fingerprints from Alvin Karpis after ridge removal by an underground physician © Rights see appendix.

3. Qualitative Evaluation

What other aspects are relevant for evaluating biometric authentication?

Operational Scenarios

Evaluation depends on the specific usage scenario.

Scenario 1: Match against database

- I have a database of biometric signals and a particular biometric signal.
- Find the identity of the person with the particular biometric signal.

Scenario 2: Match against claimed identity

- I have a single biometric signal and a particular biometric signal.
- Does the particular signal match the given signal?

Criteria (1)

Rendering of the signal may be problematic:

- Is it easy to render a biometric signal?
- Is it socially accepted to render the signal in public?
- Is it hygienic to render a biometric signal?
- Eg: Fingerprint: Touch an unhygienic surface.
- Eg: Iris, retina: Place your eye next to a sensor.
- Eg: DNA: Render body material.

Psychology of rendering:

- Rendering fingerprints associated with criminal suspicion.
- Has recently improved due to use in mobile phones.

Criteria (2)

Side Channel Information

- What additional information is contained in the biometric signal?
- Think of: Health data, genomic data, stress level.

Not Cancelable

- Biometric authentication cannot be canceled or renewed.
- If your biometric signals are publicly known you are "spoiled" for this authentication.

Criteria (3)

User control:

- Is rendering of the signal under control of the user?
- Can signal be obtained without user knowledge?
- Yes: Fingerpint (on a glass at a public discussion)
- Yes: Iris (on a public camera)
- No: Retina pretty well protected!

Forced rendering:

- Can user be forced to render signal against his will.
- Yes: Fingerprint (force finger on sensor)
- No: Retina.

Criteria (4)

Fake rendering:

- Is fake rendering of a signal possible?
- Yes: Fingerprint (use a latex copy of a finger)
- No: Fingerprint (with live-detection)
- Yes: Iris (using a static image)
- No: Iris (when pupillary reflexes are checked)

Signal Comparison:

- How complex is the algorithm?
- How trustworthy is the algorithm?
- Are biometric templates possible?

Perspectives

Continuous monitoring:

- Check biometric signals throughout a transaction.
- Continuously monitor if still the same person is using the device.

Multimodal biometrics:

- Use several biometric factors together to improve accuracy.

Adaptive Authentication

Biometrics as one additional factor of multifactor authentication.

Concept: Error-prone biometrics as sole & quick authentication for

- low trust situations (eg. up to 20 Euros)
- short time situations (eg: need hard factor every 24 hours)

Have recourse to **additional factor**

- in high trust situations
- every 24 hours or after reboot

Conclusion

Despite continuous improval and improving dissemination biometric remains problematic as a sole authentication factor.

4. Attacks

Which forms of attacks against biometric authentication are there?

How can we protect against these attacks?

Duplication Attacks

Biometric signals can be rendered by **fakes and duplicates:**

- Eg: Fingerprint: Latex copy of the finger.
- Eg: Facial recognition: Picture or facial mask.
- Eg: Iris: Picture.

Example: A fingerprint can be copied rather easily:

- Anleitung zum Kopieren eines Fingerabdrucks
- Nutzung des kopierten Fingerabdrucks
- Artikel von Heise
- Fingerprint of Wolfgang Schäuble

Rendering Attacks

Forced rendering attack:

- Attacker forces carrier to render biometric signal **against** his will.
- Eg: Ask for rendering of signal while gun pointed to head of carrier.
- Eg: Press finger against sensor using force.
- **Defense:** Alarm finger. Use particular finger to invoke silent alarm.

Unvoluntary rendering attack:

- Attacker causes carrier to render biometric signal **without** his will.
- Eg: Point facial recognition camera on sleeping person.

Mutilation Attacks

Body mutilation attack:

- Stealing the body part needed for rendering the biometric signal.
- Eg: Stealing a finger

Systemic Attacks

Many different forms:

- Render signal from duplicated sample.
- Replay attack on path from sensor to processor.
- Attack the electronic pathway where the processor communicates match or non-match
- Attack store of biometric signals to construct spoofed biometrics
- Attack store of biometric signals to learn signal to be injected after the sensor
- Attack the store of the biometric signal to upload a fake signal

5. Trust

Why would we entrust somebody else to store our biometric signals?

What About Trust?

Would users trust companies offering biometric authentication?

Customer confidence varies by industry, with 51 percent believing banks would manage biometric data securely and 45 percent confident that the government would do the same. However, just 12 percent think social media companies would be so trustworthy.

Cited from https://securityintelligence.com/news/biometric-authentication-tapping-the-trust-factor/

Trust Aspects

Question: Trusting Facebook

- not to track even if they easily could? (eg: keystroke dynamics)
- offer a possibility to log on to a non-real name account?
- offer a possibility to log on in a do-not-track manner?
- offer a possibility for anonymous but authenticated log-on?
- to properly store biometric signals, safe against third-party attackers?
- Given that Facebook earlier stored passwords in plaintext: , , ,

Increasing Trust (1)

Biometric Templates

- A kind of biometric "hash".
- Store only a subset of the biometric signal, as required for authentication.
- Reconstructing any original leading to the same template should be complicated.
- See: Excellent description of use of biometric templates in fingerprinting.

Tamper proof hardware:

- Do signal sensing, matching & template store in tamperproof hardware.
- Do enrollment in controlled environment.
- Guard access to the raw biometric signal.

Increasing Trust (2)

Trusted entities:

- A trusted entity (Trent, Microsoft, government, blockchain, whatever etc.) maintains biometric database.
- Handout of authentication results via signed certificates of identity.
- Also allows pseudonymous authentication.

6. Case Studies

Touch ID and Face ID as two examples of contemporary biometric technologies.

Case Study: Touch Id

1. Apple on Touch ID Technology
2. Apple on Touch ID Security
3. Apple on Secure Enclave
4. W on Touch ID
5. Report on hacking Touch ID

Case Study: Face Id

1. Apple on Face ID Technology
2. Apple on Face ID Security
3. Apple on Secure Enclave
4. W on Face ID
5. Face ID unable to distinguish twins
6. Hacking Face ID Open Eye Feature
7. Trying to Hack Face ID
8. Attempts to Hack Face ID
9. Unlocking iPhone X Face ID with a Mask

Appendix

Contents of Appendix

List of Figures (1/2)

List of Tables

List of Rights (1/2)

Fig. 1 Source: https://commons.wikimedia.org/wiki/File:Hand_Geometry_and_Measurements.jpg, Z22, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0

Fig. 2 Source: https://commons.wikimedia.org/wiki/File:Hand_Geometry_Reading_Device.jpg, Z22, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0

Fig. 3 Source: https://commons.wikimedia.org/wiki/File:Fingerprint_detail_on_male_finger_in_T%C5%99eb%C3%AD%C4%8D,_T%C5%99eb%C3%AD%C4%8D_District.jpg, By Frettie - Own work, CC BY 3.0, CC BY-SA 3.0 https://creativecommons.org/licenses/by-sa/3.0

Fig. 4 Sources: https://upload.wikimedia.org/wikipedia/commons/4/49/Fingerprint_Whorl.jpg, https://upload.wikimedia.org/wikipedia/commons/c/c5/Fingerprint_Arch.jpg, https://upload.wikimedia.org/wikipedia/commons/0/06/Fingerprint_Loop.jpg. Public domain as US government work.

Fig. 5 Source: https://commons.wikimedia.org/wiki/File:3D_face.stl. Cicero Moraes, CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0

Fig. 6 Source: https://commons.wikimedia.org/wiki/File:A_blue_eye.jpg, 8thstar, CC BY-SA 3.0 http://creativecommons.org/licenses/by-sa/3.0/.

Fig. 7 Source: https://upload.wikimedia.org/wikipedia/commons/3/37/Fundus_photograph_of_normal_right_eye.jpg, Mikael Häggström, Medical Gallery. WikiJournal of Medicine 1 (2), public domain.

Fig. 8 Source: https://www.medcalc.org/manual/roc-curves.php

Fig. 9 Source: https://www.medcalc.org/manual/roc-curves.php

Fig. 10 Source: https://commons.wikimedia.org/wiki/File:Roc-draft-xkcd-style.svg, MartinThoma, CC0, via Wikimedia Commons

Fig. 11 Source: https://multimedia.fbi.gov/original/3159, Public domain as US government work.

Terms of Use (1)

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt für mich ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status ich nicht oder nur mit unverhältnismäßig hohem Aufwand abklären kann. Ebenso kann ich den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen lassen, obwohl ich – und in letzter Konsequenz Sie als Leser – ihre Leistungen nutzen.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungssystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungssysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Biometric Authentication. Electronic document. https://iuk.one/1033-1009 19. 5. 2021.

Bibtex Information: https://iuk.one/1033-1009.bib

```
@misc{doc:1033-1009,
   author      = {Clemens H. Cap},
   title       = {Biometric Authentication},
   year        = {2021},
   month       = {5},
   howpublished = {Electronic document},
   url         = {https://iuk.one/1033-1009}
}
```

Typographic Information:
Typeset on May 19, 2021
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

Legend:
- continuation slide
- slide without title header
- image slide