Secure Application Design

Trust

Summer 2025

Jakob Heher, www.isec.tugraz.at
he/his

"Local fisherman in the lake surrounding the Buddhist Neak Pean temple, near Siem Reap, Cambodia", by Álvaro Bueno, thenounproject.com

A, E, I, O, U

1, 3, 5, 7, 9

RULE: If it has a *vowel* on one side, then it **must** have an *odd number* on the other side.

Which cards do I need to flip over to verify that the rule is followed?

Cosmides, L., & Tooby, J. (1992). Cognitive adaptations for social exchange. The adapted mind: Evolutionary psychology and the generation of culture, 163, 163-228.

Drinking: Water	Drinking: Beer	Age: 21 years	Age: 15 years

RULE: If you drink *Beer*, you **must** be at least *16 years* old.

Which cards do I need to flip over to verify that the rule is followed?

Cosmides, L., & Tooby, J. (1992). Cognitive adaptations for social exchange. The adapted mind: Evolutionary psychology and the generation of culture, 163, 163-228.

RULE: If it has a *vowel* on one side, then it **must** have an *odd number* on the other side.

Which cards do I need to flip over to verify that the rule is followed?

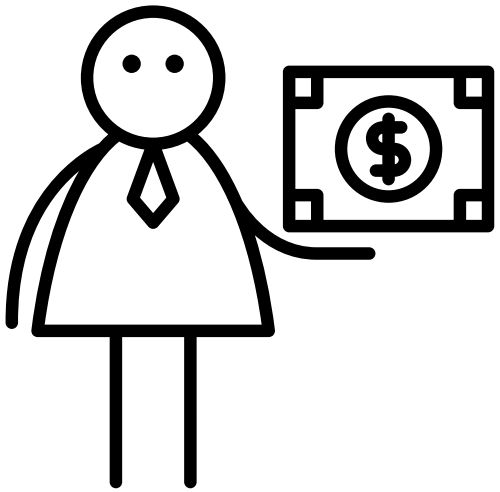
Cosmides, L., & Tooby, J. (1992). Cognitive adaptations for social exchange. The adapted mind: Evolutionary psychology and the generation of culture, 163, 163-228.

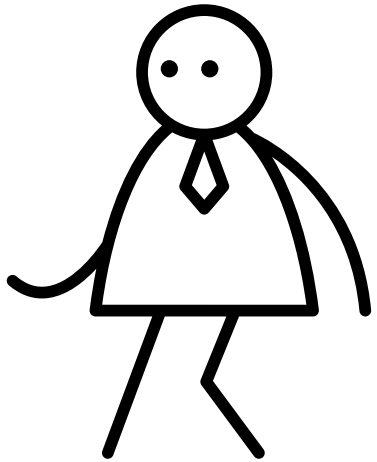
RULE: If you drink *Beer*, you **must** be at least *16 years* old.

Which cards do I need to flip over to verify that the rule is followed?

Cosmides, L., & Tooby, J. (1992). Cognitive adaptations for social exchange. The adapted mind: Evolutionary psychology and the generation of culture, 163, 163-228.

The Importance of Identifiability





So, what is “trust”?

- Trust is:
  - expecting someone to meet *commitments* they have made
  - based on our assessment of someone’s *trustworthiness*
  - required to make ourselves function within society

- We assess trustworthiness based on:
  - Someone’s *capability* to do the thing they are committing to
  - Someone’s *incentive* to do the thing they are committing to

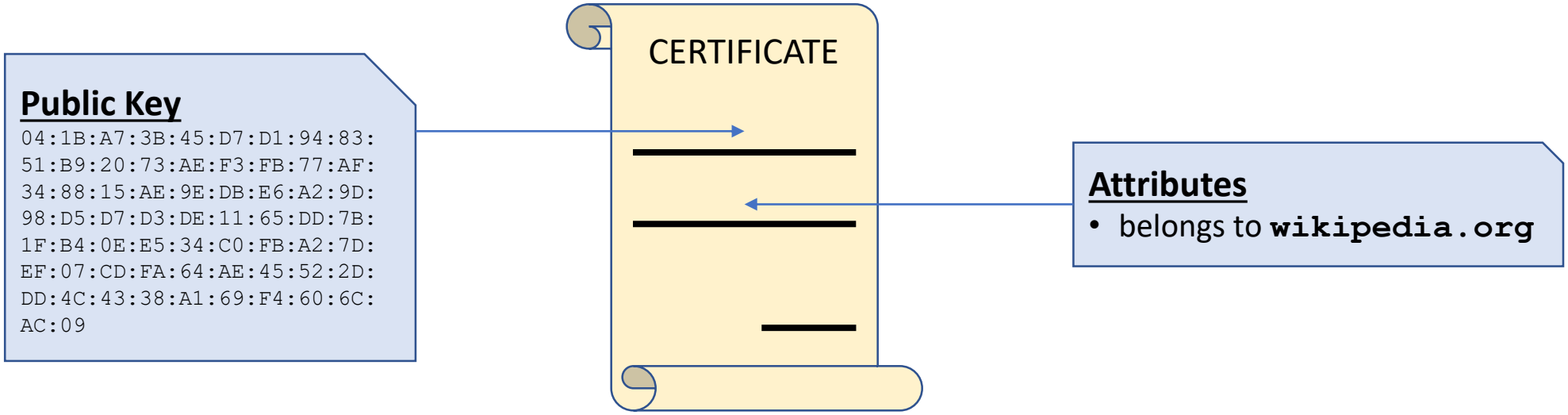
So, what is “trust”?

- Trust is:
  - expecting someone to meet commitments they have made
  - based on our assessment of someone’s *trustworthiness*
  - required to make ourselves function within society

- We can *delegate* trust decisions
  - i.e., we trust someone else to make trust decisions on our behalf
  - we can differentiate between *direct* trust and *indirect* trust

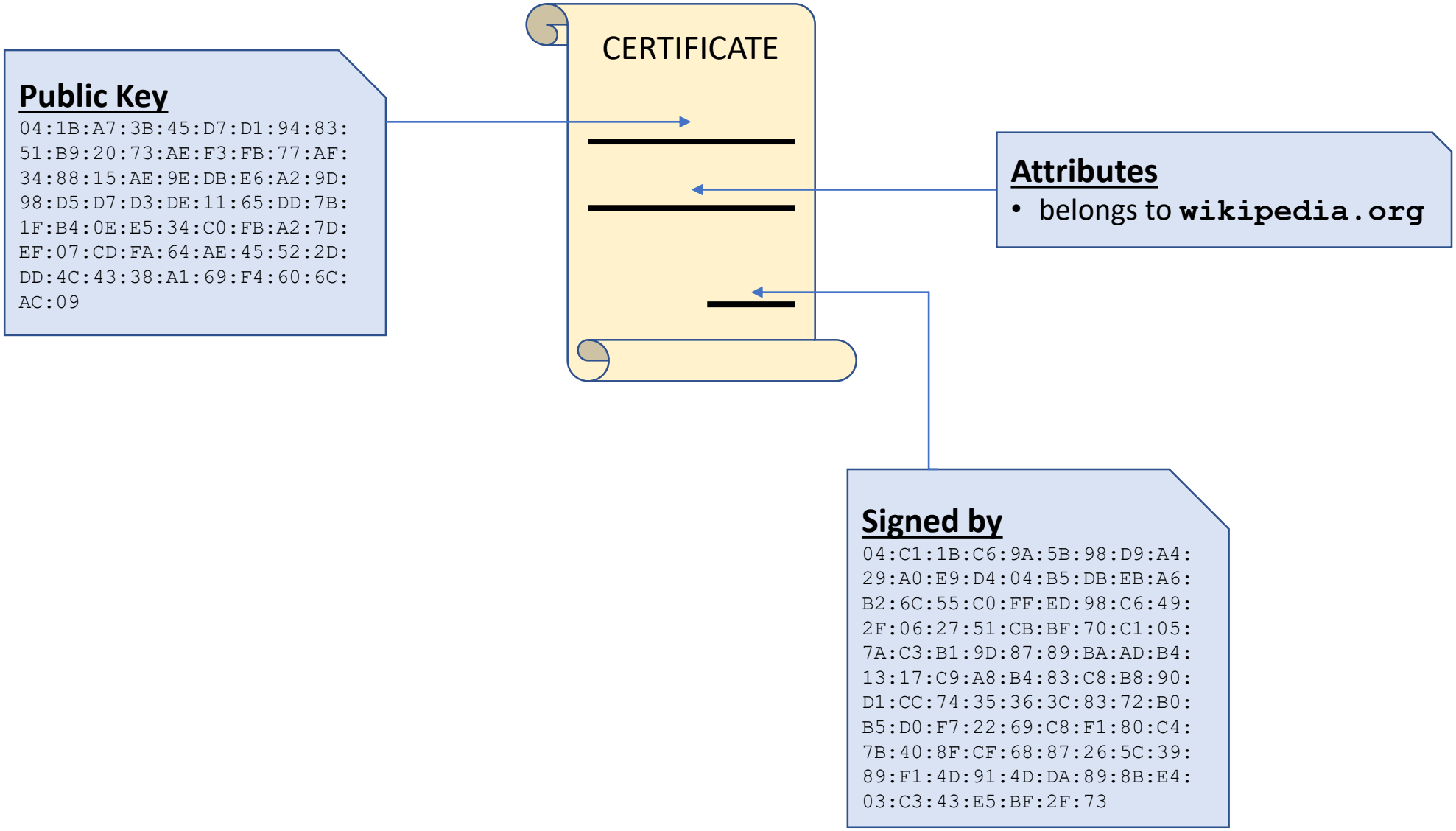
Trust in Computer Science

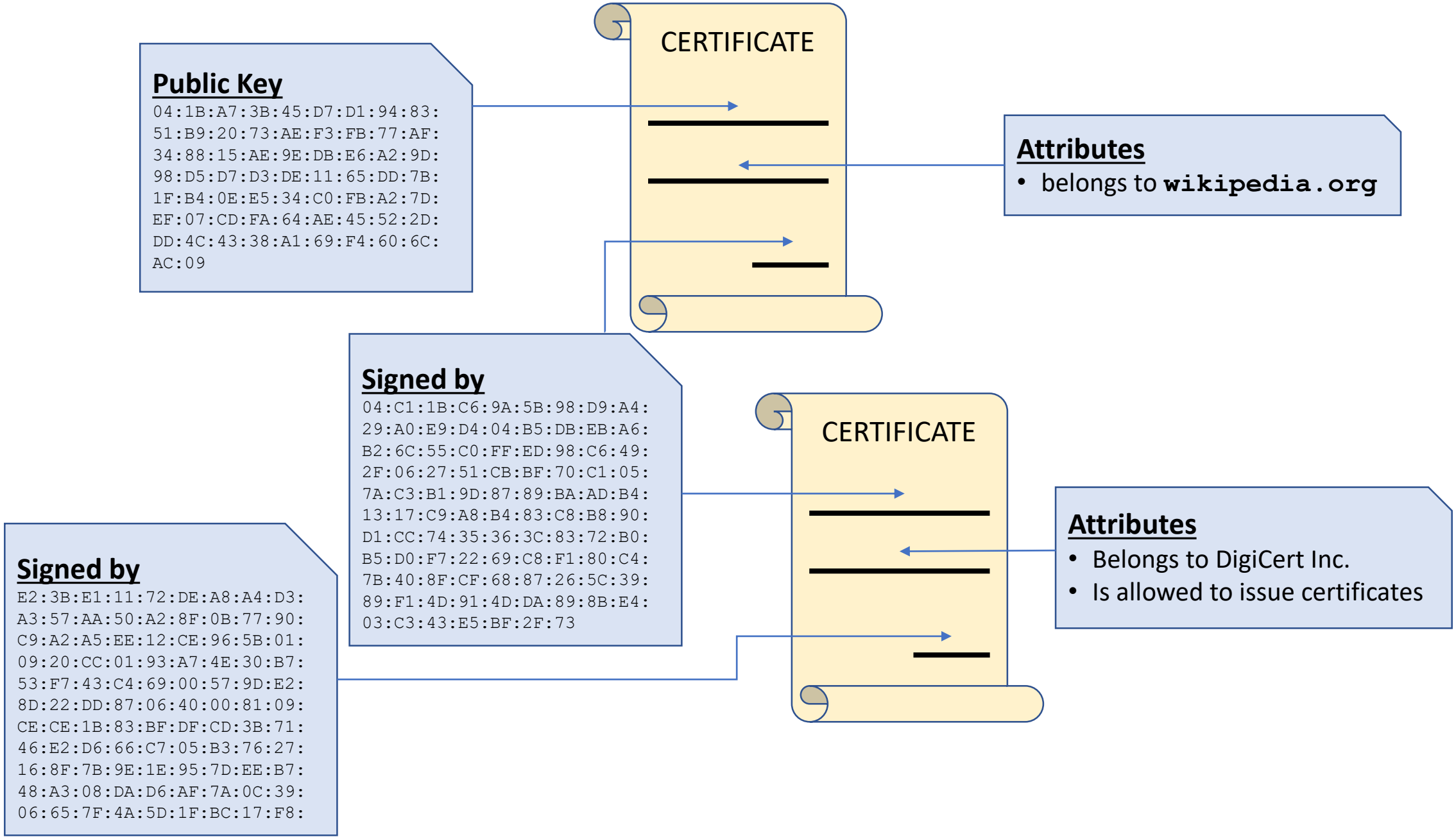
- Cryptography allows us to *prove* knowledge of a certain number
  - This number is called a *key*
- But: what does it *mean* to know that number?
- We want to *bind* certain attributes to a particular (public) key!
  - Possession of the private key ≙ proof that these attributes are met


Public Key
04:1B:A7:3B:45:D7:D1:94:83:
51:B9:20:73:AE:F3:FB:77:AF:
34:88:15:AE:9E:DB:E6:A2:9D:
98:D5:D7:D3:DE:11:65:DD:7B:
1F:B4:0E:E5:34:C0:FB:A2:7D:
EF:07:CD:FA:64:AE:45:52:2D:
DD:4C:43:38:A1:69:F4:60:6C:
AC:09
CERTIFICATE
Attributes
• belongs to wikipedia.org

Trust in Computer Science

- Cryptography allows us to *prove* knowledge of a certain number
  - This number is called a *key*
- But: what does it *mean* to know that number?
- We want to *bind* certain attributes to a particular (public) key!
  - Possession of the private key ≙ proof that these attributes are met
- But: who do we trust to make this binding?


CERTIFICATE
Public Key
04:1B:A7:3B:45:D7:D1:94:83:
51:B9:20:73:AE:F3:FB:77:AF:
34:88:15:AE:9E:DB:E6:A2:9D:
98:D5:D7:D3:DE:11:65:DD:7B:
1F:B4:0E:E5:34:C0:FB:A2:7D:
EF:07:CD:FA:64:AE:45:52:2D:
DD:4C:43:38:A1:69:F4:60:6C:
AC:09
Attributes
• belongs to wikipedia.org
Signed by
04:C1:1B:C6:9A:5B:98:D9:A4:
29:A0:E9:D4:04:B5:DB:EB:A6:
B2:6C:55:C0:FF:ED:98:C6:49:
2F:06:27:51:CB:BF:70:C1:05:
7A:C3:B1:9D:87:89:BA:AD:B4:
13:17:C9:A8:B4:83:C8:B8:90:
D1:CC:74:35:36:3C:83:72:B0:
B5:D0:F7:22:69:C8:F1:80:C4:
7B:40:8F:CF:68:87:26:5C:39:
89:F1:4D:91:4D:DA:89:8B:E4:
03:C3:43:E5:BF:2F:73


Public Key
04:1B:A7:3B:45:D7:D1:94:83:
51:B9:20:73:AE:F3:FB:77:AF:
34:88:15:AE:9E:DB:E6:A2:9D:
98:D5:D7:D3:DE:11:65:DD:7B:
1F:B4:0E:E5:34:C0:FB:A2:7D:
EF:07:CD:FA:64:AE:45:52:2D:
DD:4C:43:38:A1:69:F4:60:6C:
AC:09
CERTIFICATE
Attributes
• belongs to wikipedia.org
Signed by
04:C1:1B:C6:9A:5B:98:D9:A4:
29:A0:E9:D4:04:B5:DB:EB:A6:
B2:6C:55:C0:FF:ED:98:C6:49:
2F:06:27:51:CB:BF:70:C1:05:
7A:C3:B1:9D:87:89:BA:AD:B4:
13:17:C9:A8:B4:83:C8:B8:90:
D1:CC:74:35:36:3C:83:72:B0:
B5:D0:F7:22:69:C8:F1:80:C4:
7B:40:8F:CF:68:87:26:5C:39:
89:F1:4D:91:4D:DA:89:8B:E4:
03:C3:43:E5:BF:2F:73
CERTIFICATE
Attributes
• Belongs to DigiCert Inc.
• Is allowed to issue certificates
Signed by
E2:3B:E1:11:72:DE:A8:A4:D3:
A3:57:AA:50:A2:8F:0B:77:90:
C9:A2:A5:EE:12:CE:96:5B:01:
09:20:CC:01:93:A7:4E:30:B7:
53:F7:43:C4:69:00:57:9D:E2:
8D:22:DD:87:06:40:00:81:09:
CE:CE:1B:83:BF:DF:CD:3B:71:
46:E2:D6:66:C7:05:B3:76:27:
16:8F:7B:9E:1E:95:7D:EE:B7:
48:A3:08:DA:D6:AF:7A:0C:39:
06:65:7F:4A:5D:1F:BC:17:F8:

Roots of Trust

- At some point, we still need to *trust* someone!
  - No amount of cryptography will solve this

- Who do you trust to decide who you should trust?
  - Yourself?
  - Your friends?
    - Your friends' friends?
  - Government agencies?
  - Private companies?

Public Key Infrastructures in practice

- The Web PKI
  - Used for HTTPS
  - Your OS/browser ships with a built-in trust store
- eIDAS trust service infrastructure
  - Used for legally binding digital signatures
  - Single trust root (EU-LOTL signing key) specified by legislation[1]
- DNSSEC
  - Used to validate DNS results' integrity
  - Single trust root (root zone signing key)
  - Key signing ceremonies are *incredibly* quirky[2]

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2019.276.01.0001.01.ENG
[2] https://www.youtube.com/@iana-org/streams

More Thoughts on Trust

- *Liability*: where does the buck stop?
  - Influences the liable party's *incentives*
- *Certification*: someone assumes liability for someone else's capability
  - Influences our perception of the certified party's *capabilities*
- *Identifiability*: an entity's reputation is tied to a unique (?) identifier
  - How disposable is this identifier?

Secure Application Design

Privacy

Summer 2025

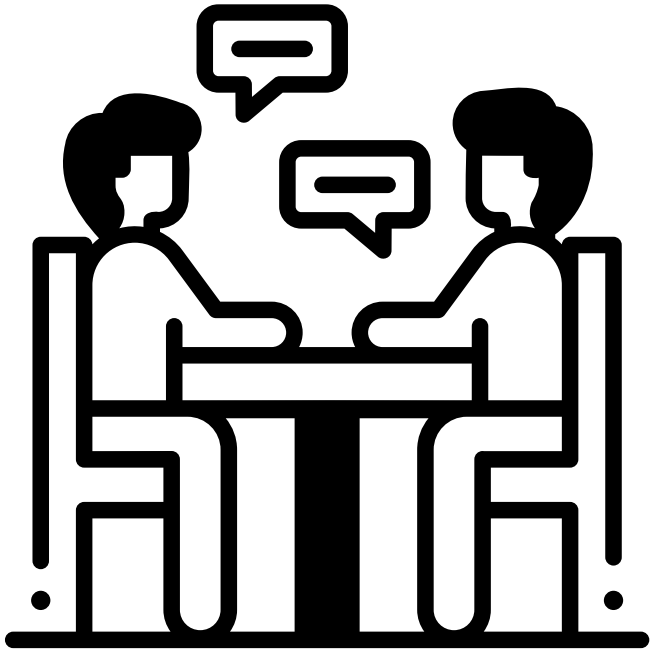
Jakob Heher, www.isec.tugraz.at
he/his

What is “Privacy”?

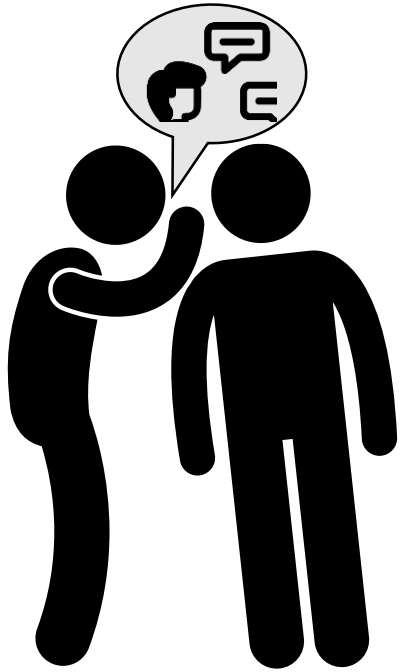
- Not being observed?
  - Being able to “be yourself” without regard for others’ expectations?
  - Not *feeling* observed?
- Not being *distinguished*?
  - Being able to blend into a crowd?
- Having control of what information others have about you?
  - Retaining control of others’ perception of you?

- All of the above and more? It’s complicated.

Privacy and Freedom of Speech

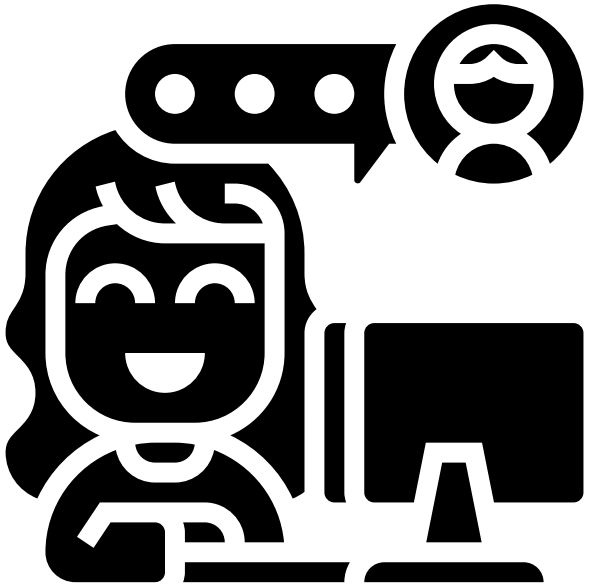


Privacy ***is necessary for*** Freedom of Speech

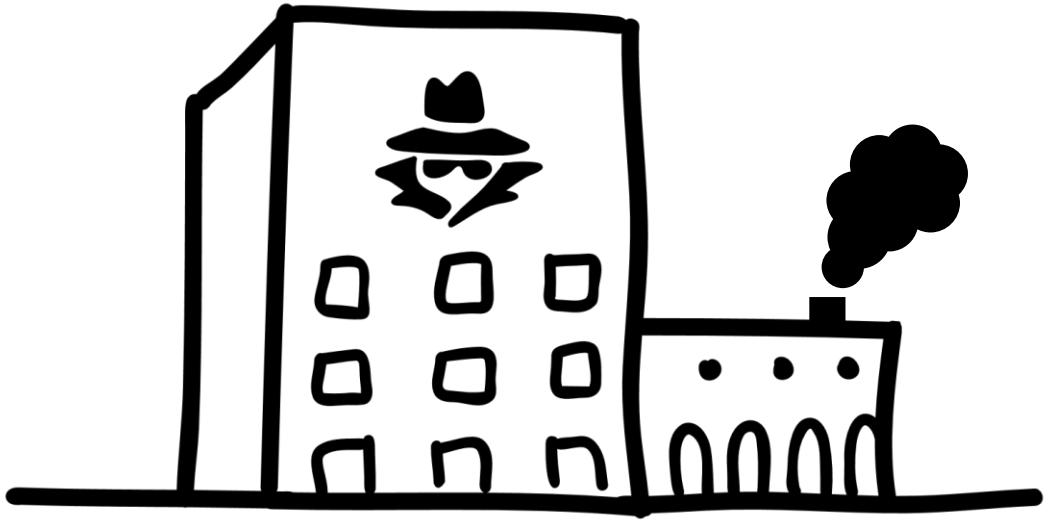


Privacy ***conflicts with*** Freedom of Speech

Privacy and Computers



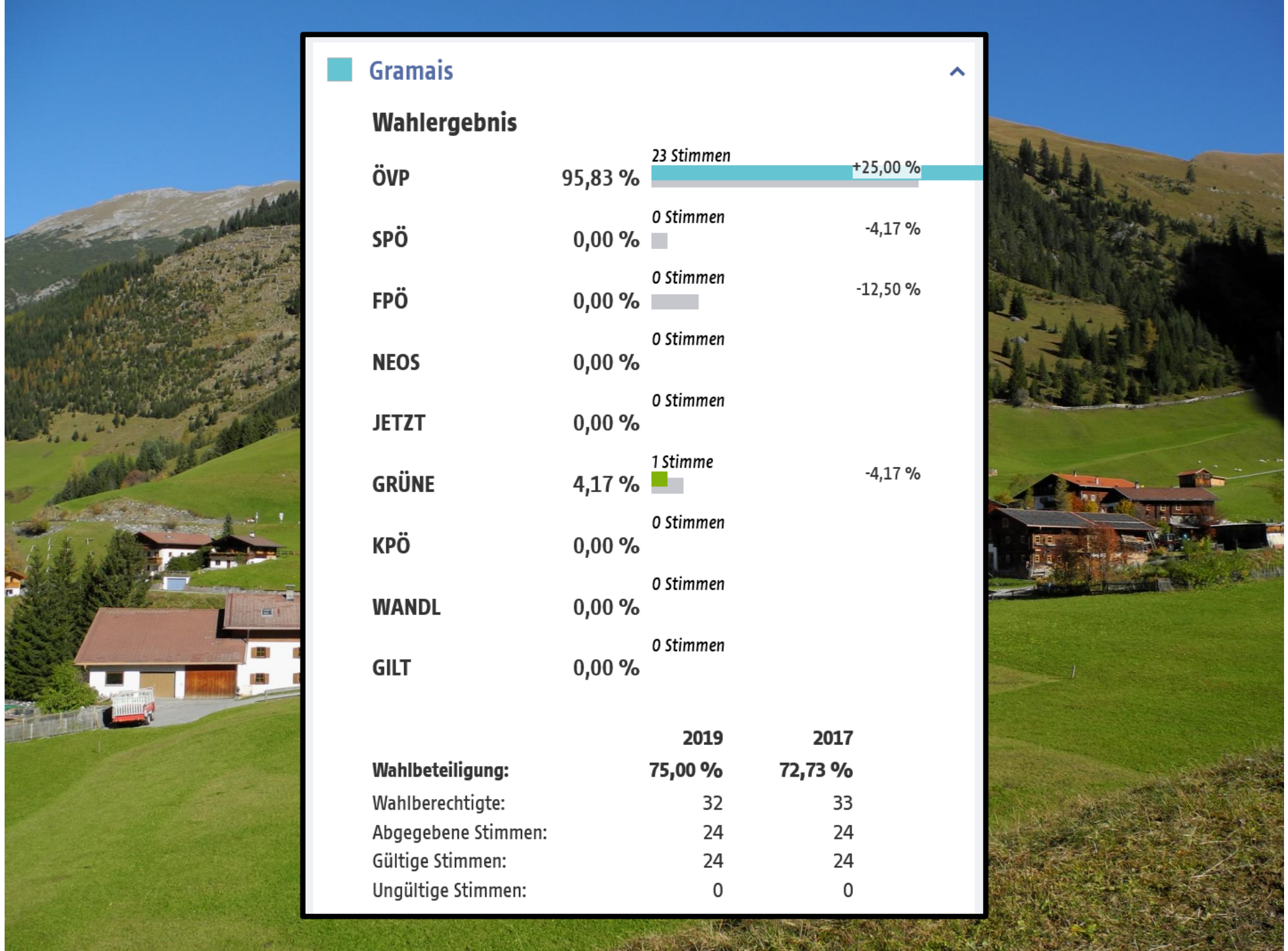
Computers ***enable*** Privacy



Computers ***endanger*** Privacy

Privacy Concepts in Computer Science

- *Anonymity*: an action cannot be attributed to you

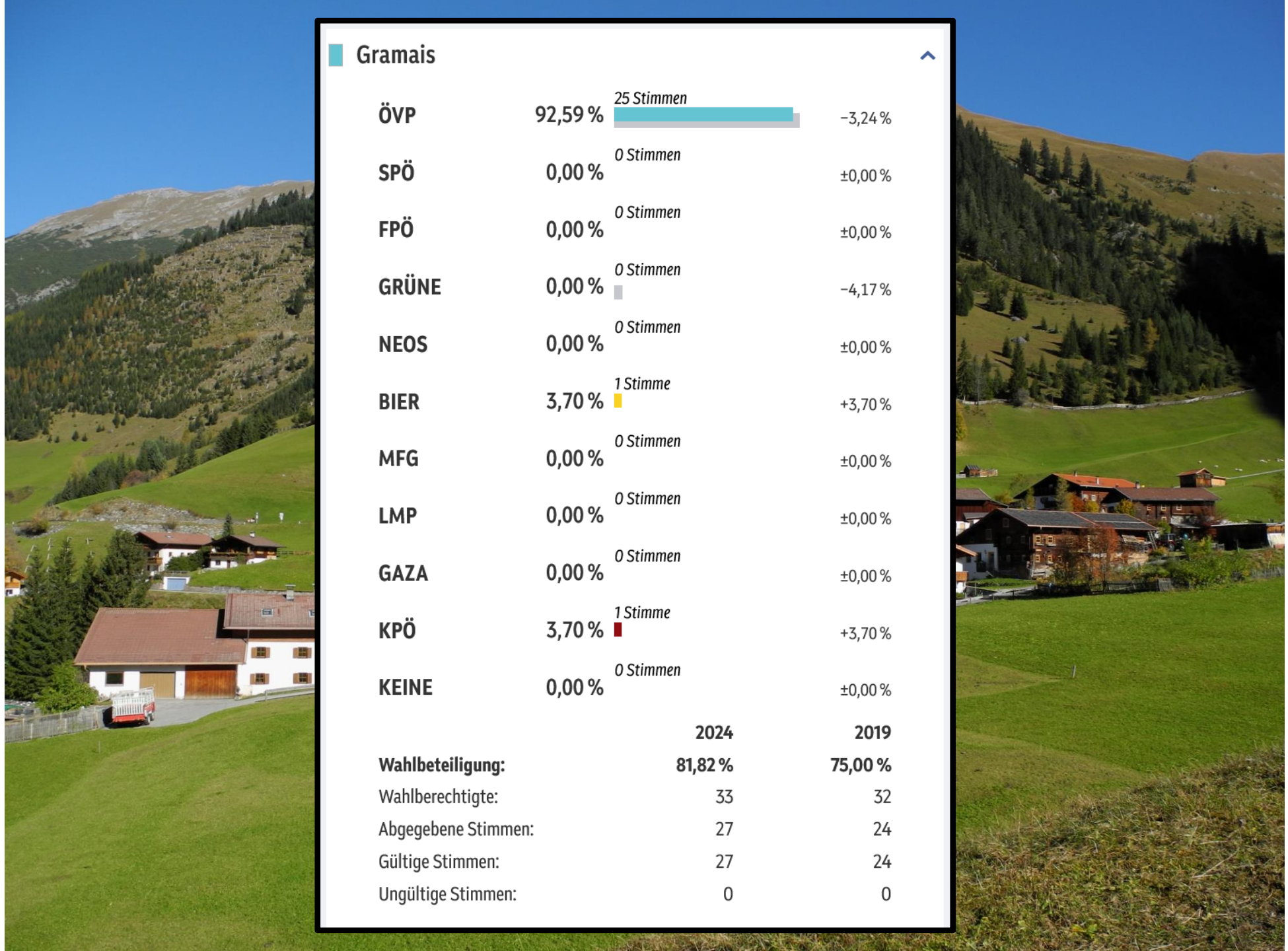


Gramais

Wahlergebnis

ÖVP	95,83 %	23 Stimmen	+25,00 %
SPÖ	0,00 %	0 Stimmen	-4,17 %
FPÖ	0,00 %	0 Stimmen	-12,50 %
NEOS	0,00 %	0 Stimmen	
JETZT	0,00 %	0 Stimmen	
GRÜNE	4,17 %	1 Stimme	-4,17 %
KPÖ	0,00 %	0 Stimmen	
WANDL	0,00 %	0 Stimmen	
GILT	0,00 %	0 Stimmen	

	2019	2017
Wahlbeteiligung:	**75,00 %**	**72,73 %**
Wahlberechtigte:	32	33
Abgegebene Stimmen:	24	24
Gültige Stimmen:	24	24
Ungültige Stimmen:	0	0



Gramais

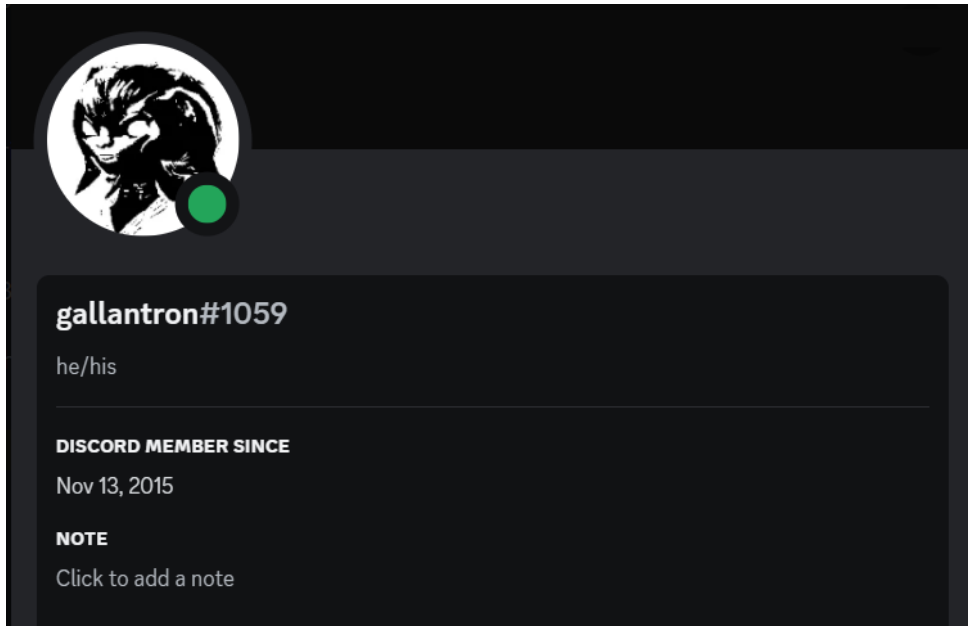
ÖVP	92,59 %	25 Stimmen	−3,24 %
SPÖ	0,00 %	0 Stimmen	±0,00 %
FPÖ	0,00 %	0 Stimmen	±0,00 %
GRÜNE	0,00 %	0 Stimmen	−4,17 %
NEOS	0,00 %	0 Stimmen	±0,00 %
BIER	3,70 %	1 Stimme	+3,70 %
MFG	0,00 %	0 Stimmen	±0,00 %
LMP	0,00 %	0 Stimmen	±0,00 %
GAZA	0,00 %	0 Stimmen	±0,00 %
KPÖ	3,70 %	1 Stimme	+3,70 %
KEINE	0,00 %	0 Stimmen	±0,00 %

	2024	2019
Wahlbeteiligung:	**81,82 %**	**75,00 %**
Wahlberechtigte:	33	32
Abgegebene Stimmen:	27	24
Gültige Stimmen:	27	24
Ungültige Stimmen:	0	0

Privacy Concepts in Computer Science

- *Anonymity*: an action cannot be attributed to you
  - You remain indistinguishable within the *anonymity set*

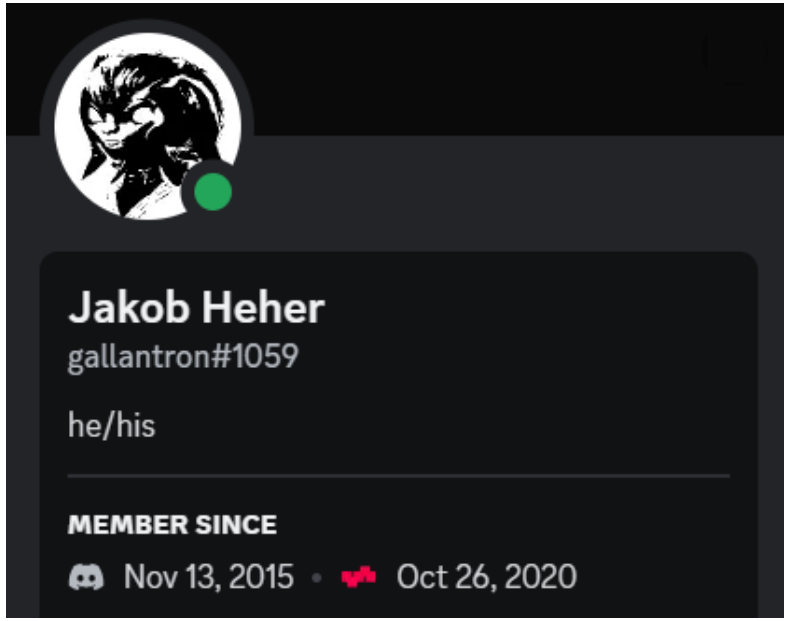
- *Pseudonymity*: an action can be attributed to a pseudonym



Privacy Concepts in Computer Science

- *Anonymity*: an action cannot be attributed to you
  - You remain indistinguishable within the *anonymity set*

- *Pseudonymity*: an action can be attributed to a pseudonym



Privacy Concepts in Computer Science

- *Anonymity*: an action cannot be attributed to you
  - You remain indistinguishable within the *anonymity set*
- *Pseudonymity*: an action can be attributed to a pseudonym
  - The pseudonym is *a priori* not linked to any other unique identifier
- *Unlinkability*: multiple actions cannot be linked to each other
- *Undetectability*: a third party cannot tell whether the action happens
- *Deniability*: nobody can prove I performed the action

Practical Example: Undetectability

- Rule 0 of credentials: Revocation is hard
- Naïve approach: long-lived credential & online revocation list
  - Problem: this makes use of credentials *detectable* to the issuer!
- Common Solution:
  - Credential holder retrieves short-lived, signed attestation of validity
  - Credential holder supplies credential + attestation of validity
  - Credential verifier can check signatures & recency

Laws about Privacy: the GDPR

- According to the GDPR, “personal data” is:
  - Any information related to an individual who can be directly or indirectly identified
- Data must be processed according to *seven principles*:
  1. Lawfulness, fairness, and transparency
  2. Purpose limitation
  3. Data minimization
  4. Accuracy
  5. Storage limitation
  6. Integrity and confidentiality
  7. Accountability

Learn more: https://gdpr.eu/what-is-gdpr/

Laws about Privacy: the GDPR

- According to the GDPR, “personal data” is:
  - Any information related to an individual who can be directly or indirectly identified
- Processing personal data must be justified by one of the below:
  1. Specific and unambiguous consent was given
  2. Processing is necessary for the preparation or execution of a contract
  3. You have a legal obligation to process the data
  4. Processing the data is required to protect vital interests
  5. Performing a task that is in the public interest, or some official function
  6. You have a legitimate interest in processing the data
     a) Unless the legitimate interest is overridden by the subject’s fundamental rights and freedoms

Learn more: https://gdpr.eu/what-is-gdpr/

Laws about Privacy: the GDPR

- According to the GDPR, “personal data” is:
  - Any information related to an individual who can be directly or indirectly identified
- Consent to data processing is subject to the following:
  - Consent must be “freely given, specific, informed, and unambiguous”
  - Requests for consent must be “clearly distinguishable from other matters”
  - Requests for consent must be presented in “clear and plain language”
  - Consent may be withdrawn at any time, and data processing must then cease
  - Children under 13 cannot consent to data processing without parental supervision
  - Data processors must keep documentary evidence of subjects’ consent

Learn more: https://gdpr.eu/what-is-gdpr/

Laws about Privacy: the GDPR

- According to the GDPR, “personal data” is:
  - Any information related to an individual who can be directly or indirectly identified
- Data subjects are afforded the following rights:
  1. Right to be informed
  2. Right of access to data
  3. Right to rectification
  4. Right to erasure
  5. Right to restriction of processing
  6. Right to data portability
  7. Right to object to processing
  8. Right to avoid automated profiling

Learn more: https://gdpr.eu/what-is-gdpr/

Threat Modeling for Privacy: LINDDUN

Linkability

An adversary is able to link two items of interest without knowing the identity of the data subject(s) involved.

Identifiability

An adversary is able to identify a data subject from a set of data subjects through an item of interest.

Non-repudiation

The data subject is unable to deny a claim (e.g., having performed an action, or sent a request).

Detectability

An adversary is able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read its contents.

Disclosure of information

An adversary is able to learn the content of an item of interest about a data subject.

Unawareness

The data subject is unaware of the collection, processing, storage, or sharing activities (and corresponding purposes) of the data subject's personal data.

Non-compliance

The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy.

Learn more: https://www.linddun.org/

Want To Know More?

- 705.054 Privacy-Enhancing Technologies
  - https://www.iaik.tugraz.at/pets
  - offered in winter semester

- Subjects covered:
  - Database recovery
  - Differential Privacy & k-anonymity
  - Traffic analysis & TOR
  - Multi-Party Computation
  - and many more…