

Grundlagen:

Verschlüsseln

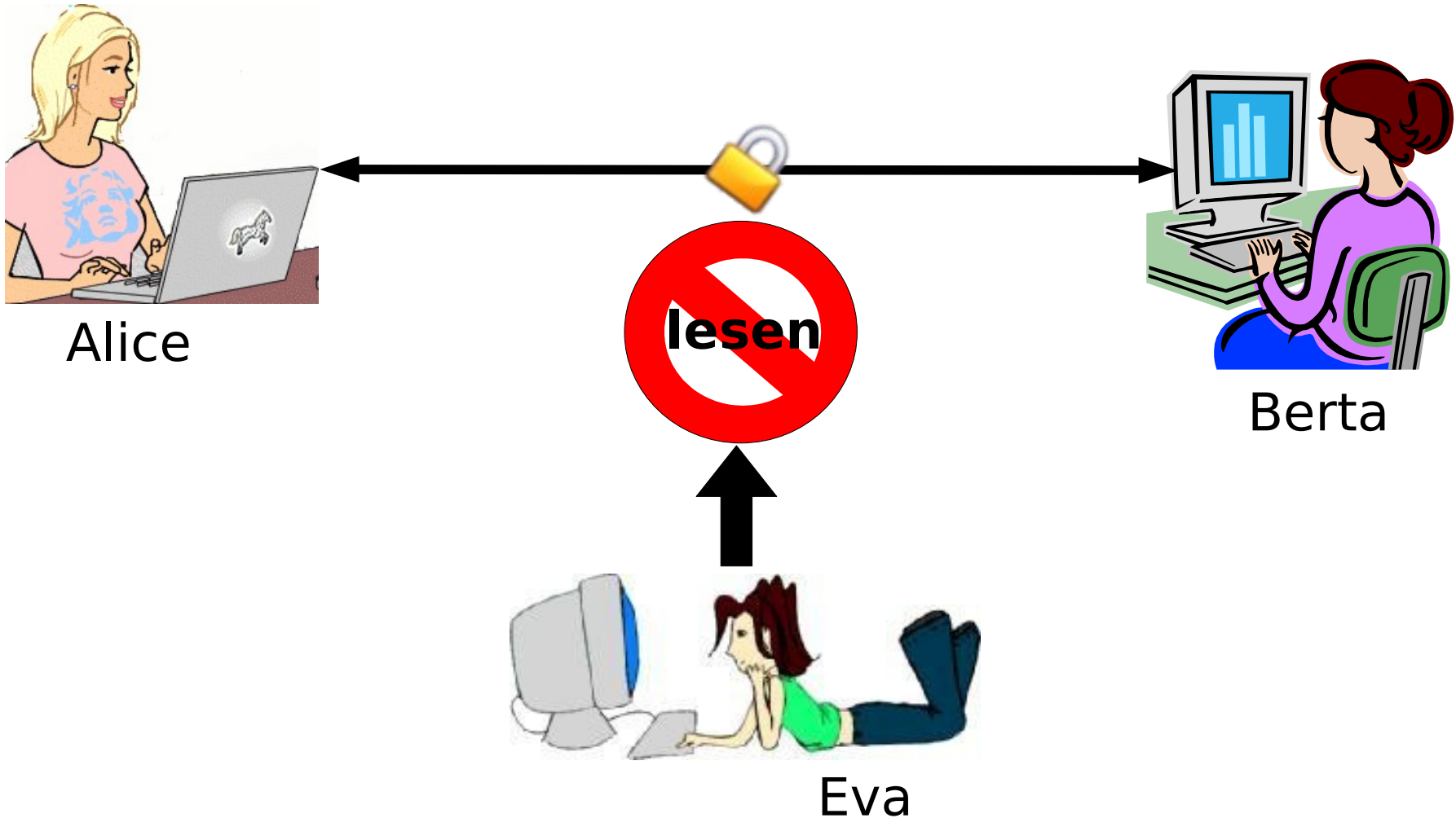
Signieren

Vertrauen

Zertifizieren

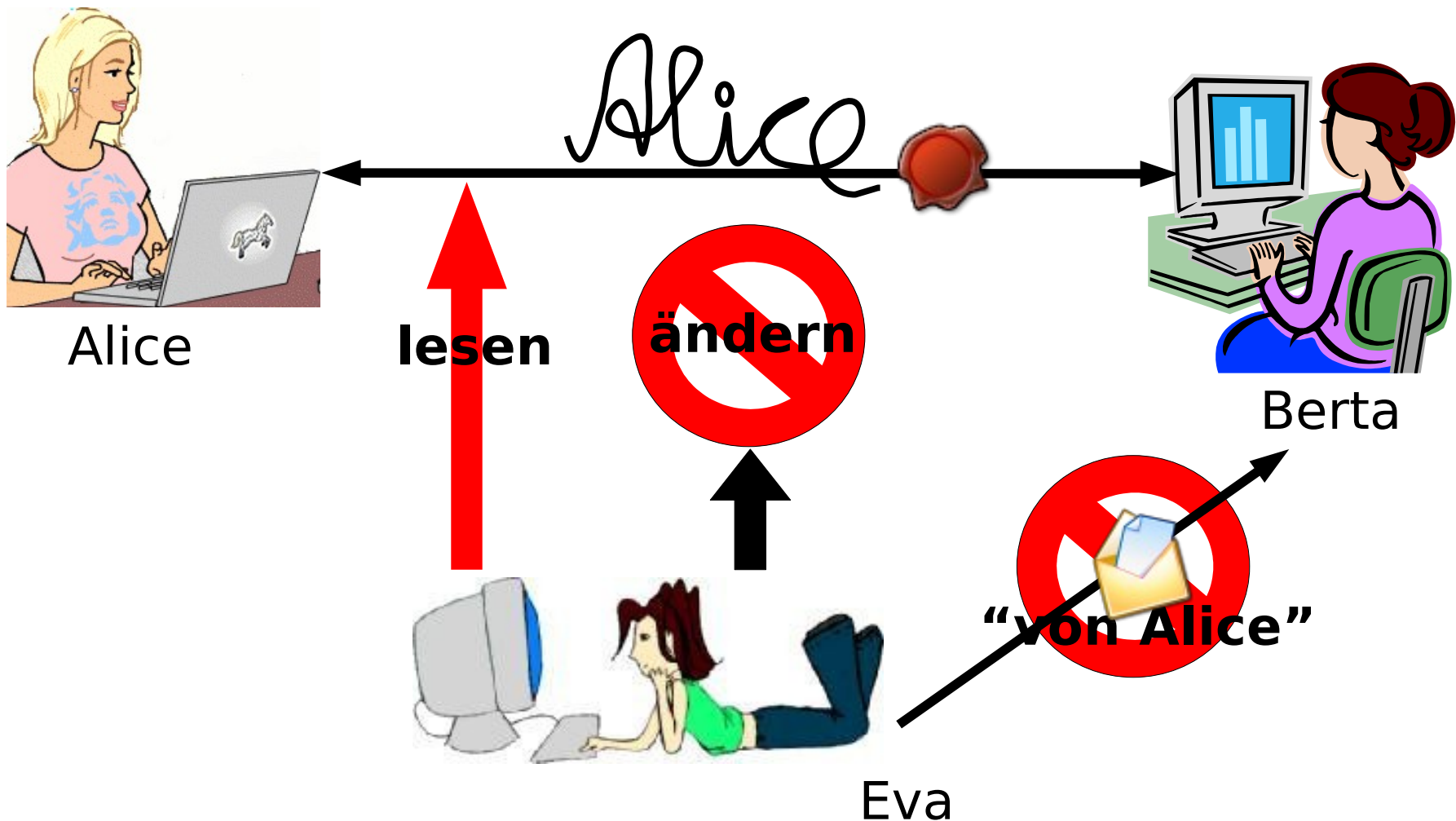
Verschlüsseln

- Übertragung von Geheimnissen

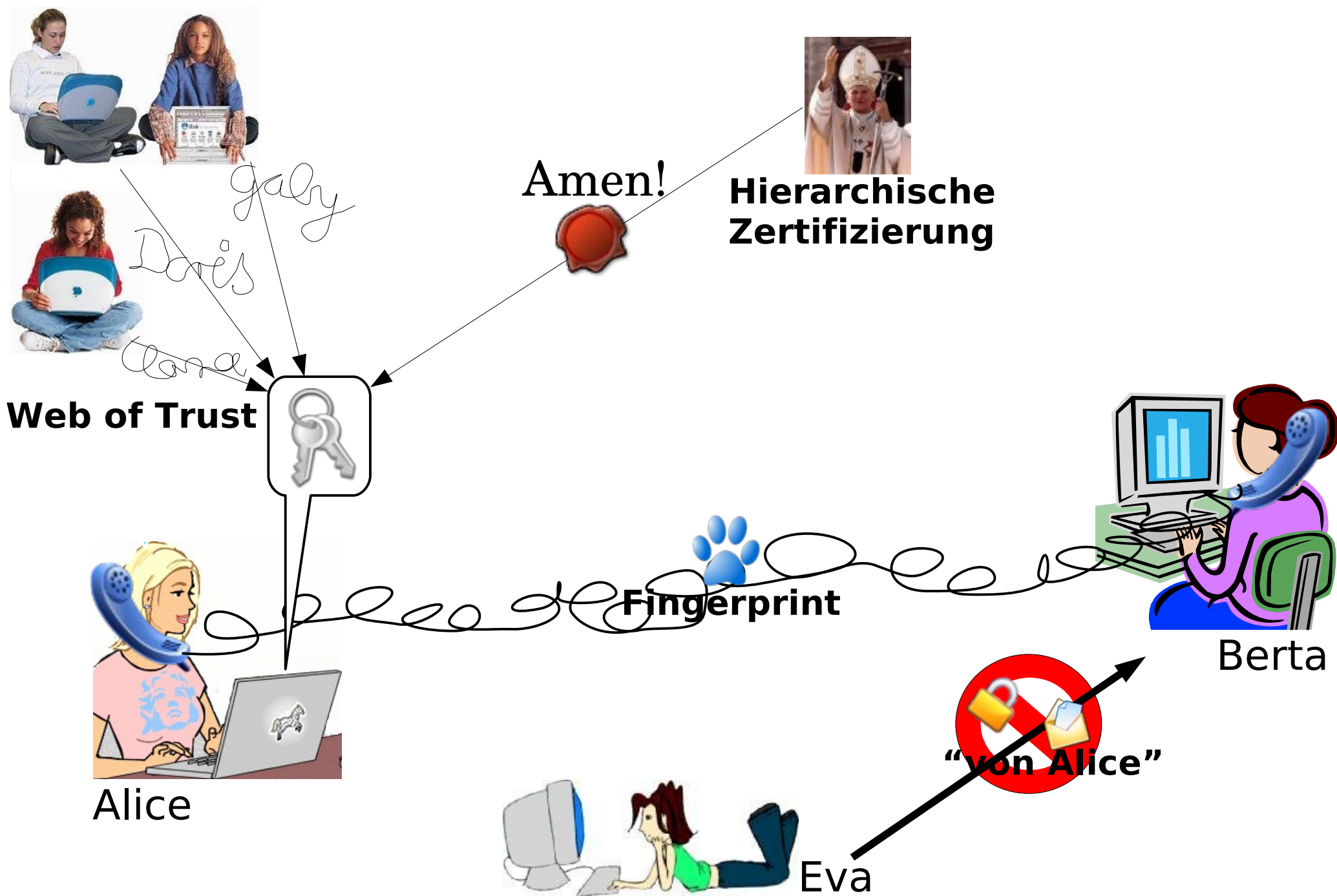


Signieren

- Gewährleistung der Authentizität des Senders, der Integrität der Nachricht (wie Siegel)



Authentizität: Ist das wirklich von Alice?



Web Of Trust

- PGP/GPG
- Key Signing Party
- ich vertraue darauf, dass der Schlüssel zu Berta gehört, weil ich Alice vertraue und Alice sagt, dass das Bertas Schlüssel ist
- Unterschiedliche Vertrauensstärken
 - Wie stark vertraut man einer Person, andere Schlüssel korrekt zu überprüfen?
 - Wie viele Personen haben diesen Schlüssel überprüft?

Zertifizierung

- Public Key Infrastructure (PKI): hierarchische Zertifizierung
- SSL, S/MIME
- Behörden oder Firmen
- zentrale Zertifizierungsinstanz

Noch Fragen?

