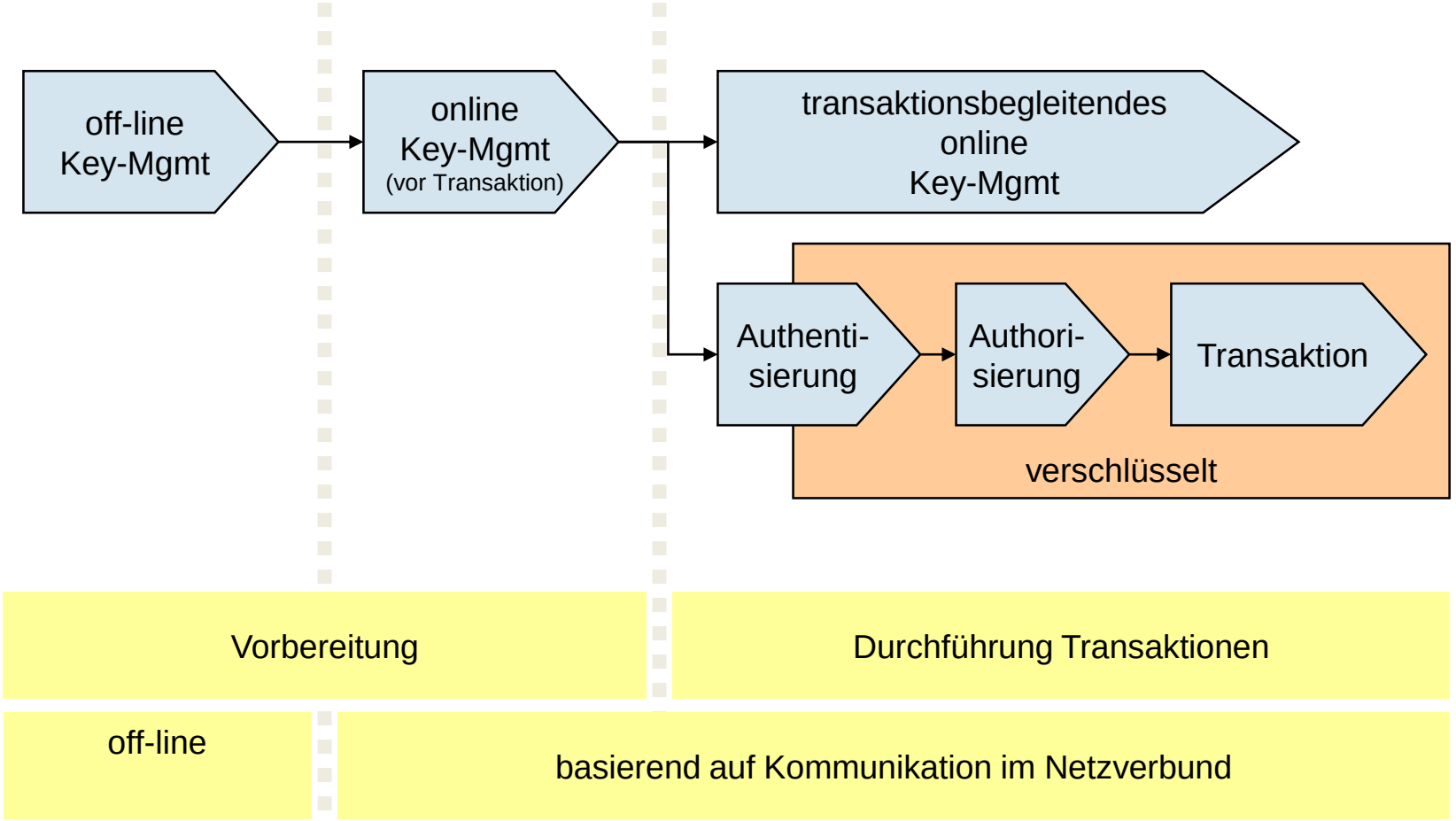
Hochschule
Bonn-Rhein-Sieg

Prof. Dr. Martin Leischner
Netzwerksysteme und TK

Sicherheit in Netzen
Modul 6: Authentisierung

1. Problemstellung, Grundarchitektur, Begriffsklärung
2. Einschub Aufbau und Funktion einer Chipkarte
3. Klassifikationsschema Authentisierung
4. Authentisierungsverfahren

Key-Management, Authentisierung und Verschlüsselung



A+A=A

Unterscheidung: Authentisierung – Autorisierung

- **Authentisierung - Prozess, bei dem ein Nutzer (allgemeiner eine Ressource) das Recht auf eine Identität begründet.**
  Schlüsselfrage: Wer bist du?

- **Autorisierung – Prozess, bei dem einer Identität (unter Einbezug einer Menge zugeordneter Attribute) die Erlaubnis erteilt wird, bestimmte Aktionen durchzuführen.**
  Schlüsselfrage: Was darfst du machen?

- **Formel: A + A = A:**
  Authentisierung + Autorisierung = Access / Accounting

Verschiedene Definitionen 'Authentisierung'

- American National Standard for Telecommunications (http://www.its.bldrdoc.gov):
  - A security measure designed to protect a communications system against acceptance of a fraudulent transmission or simulation by establishing the validity of a transmission, message, or originator.
- OASIS, the Organization for the Advancement of Structured Information Standards (http://www.oasis-open.org/committees/security)
  - Authentication is the process of confirming a system entity's (=an active element of a system - e.g., an automated process or set of processes, a subsystem, a person or group of persons--that incorporates a specific set of capabilities) asserted principal identity (= AAA Service clients) with a specified, or understood, level of confidence.
- Center for Democracy and Technology (http://www.cdt.org/)
  - Authentication - the process of verifying that a file or message has not been altered in route from the distributor to the recipient(s).

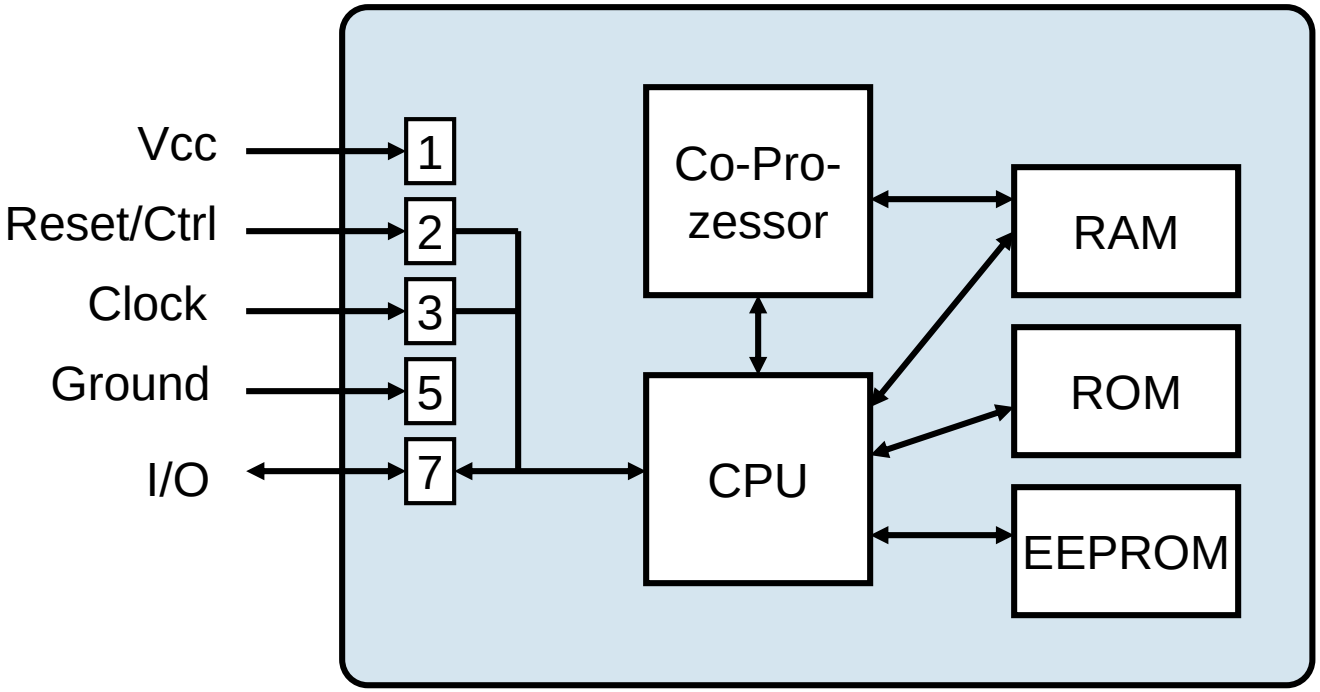
Definition 'Authentisierung' nach Clifford Lynch

- Authentication is the process where a network user establishes a right to an identity - in essence, the right to use a name.
- Validating authenticity entails verifying claims that are associated with an object - in effect, verifying that an object is indeed what it claims to be, or what it is claimed to be (by external metadata).

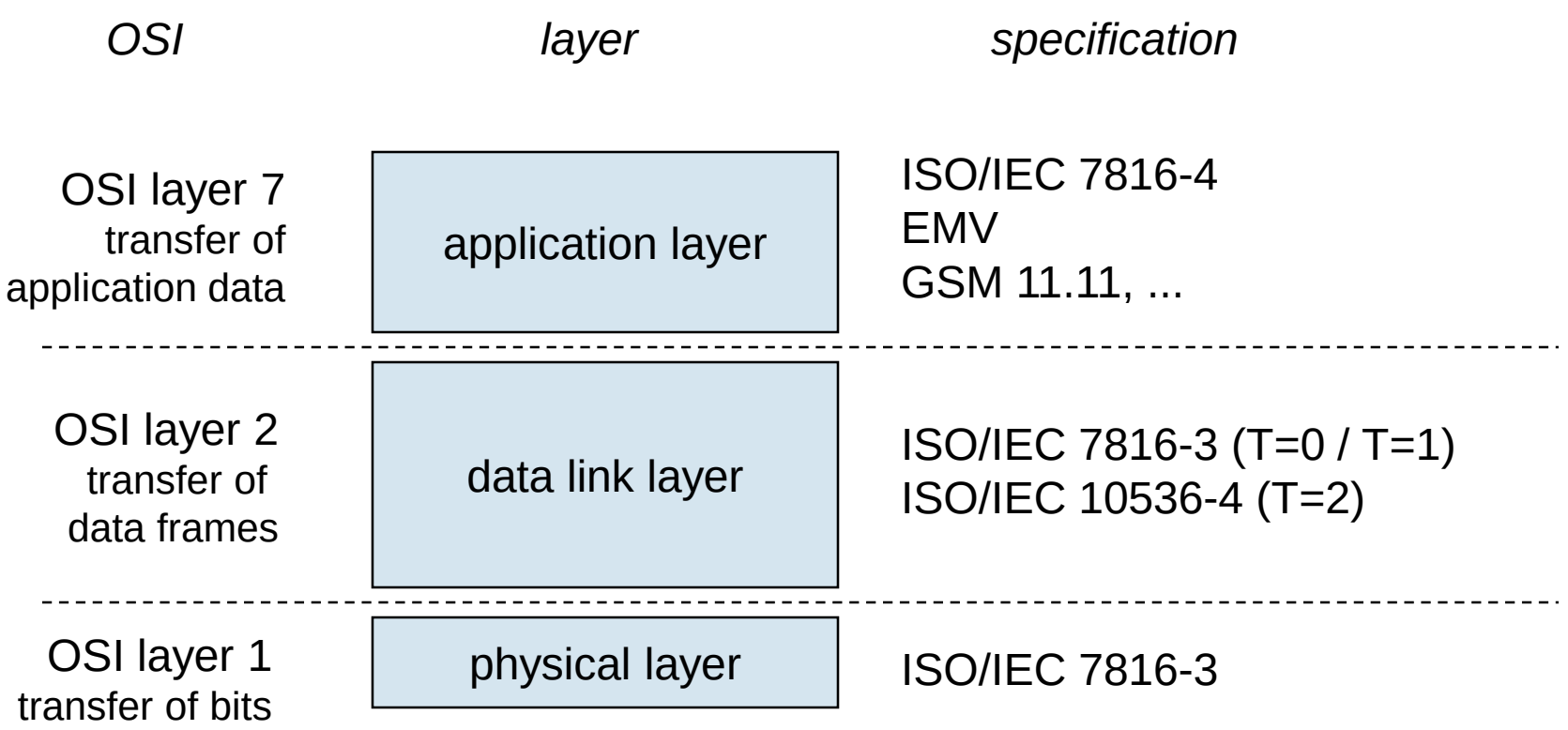
Clifford Lynch (ed.): A White Paper on Authentication and Access Management Issues in Cross-Organizational Use of Networked Information Resources, Coalition for Networked Information, Spring 1998. (Revised discussion draft – April 14).
Available at http://www.cni.org/publications/cliffs-pubs/white-paper-authentication-access-mgt-issues/ , accessed: December 1, 2013.

Lynch Clifford A.: Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust," Authenticity in a Digital Environment. Washington, DC, Council on Library and Information Resources, pp 32-50, 2000. Available at http://www.clir.org/pubs/reports/pub92/lynch.html, accessed: December 1, 2013.

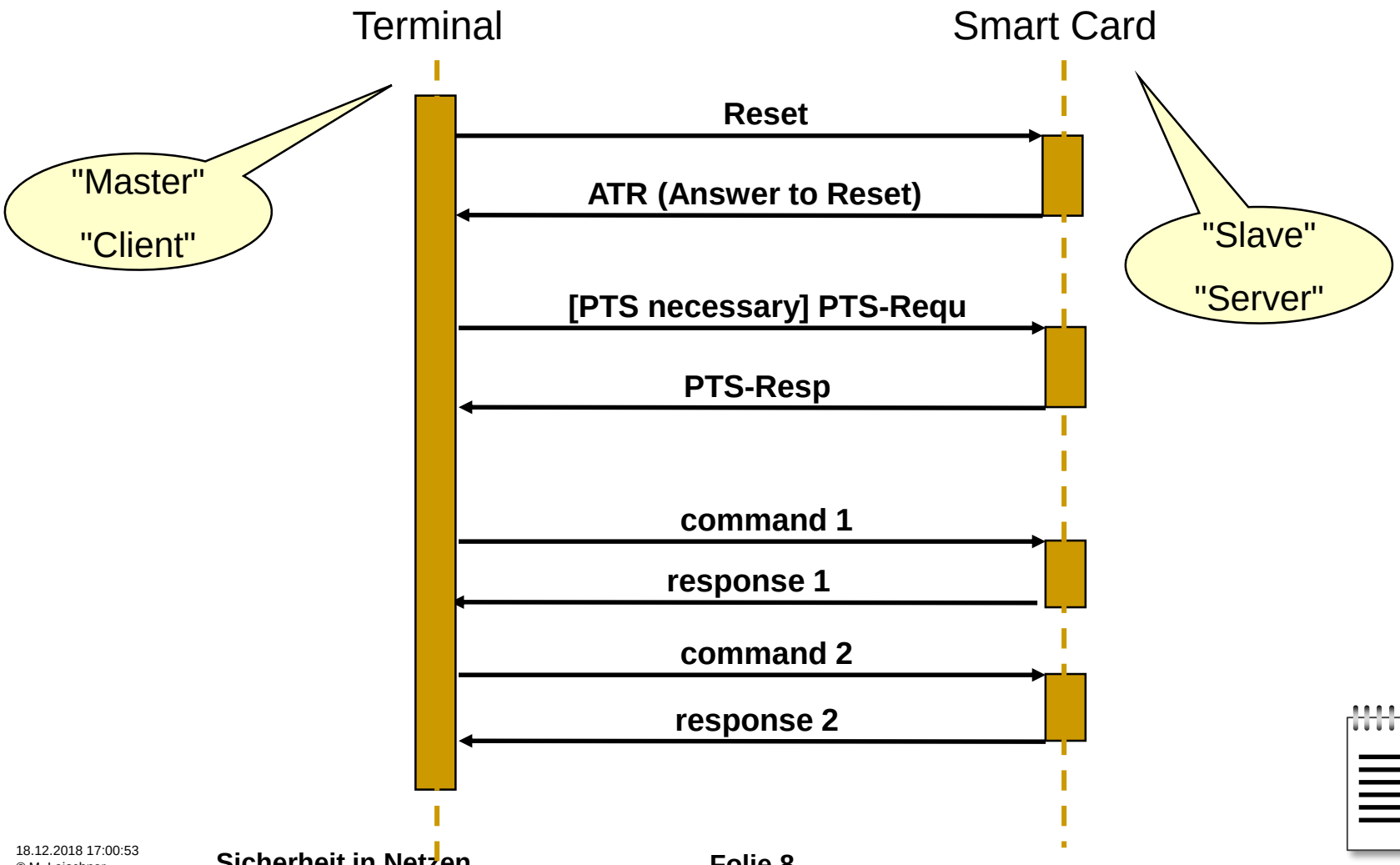
Einschub Chipkarte: Aufbau einer Prozessor-Chipkarte



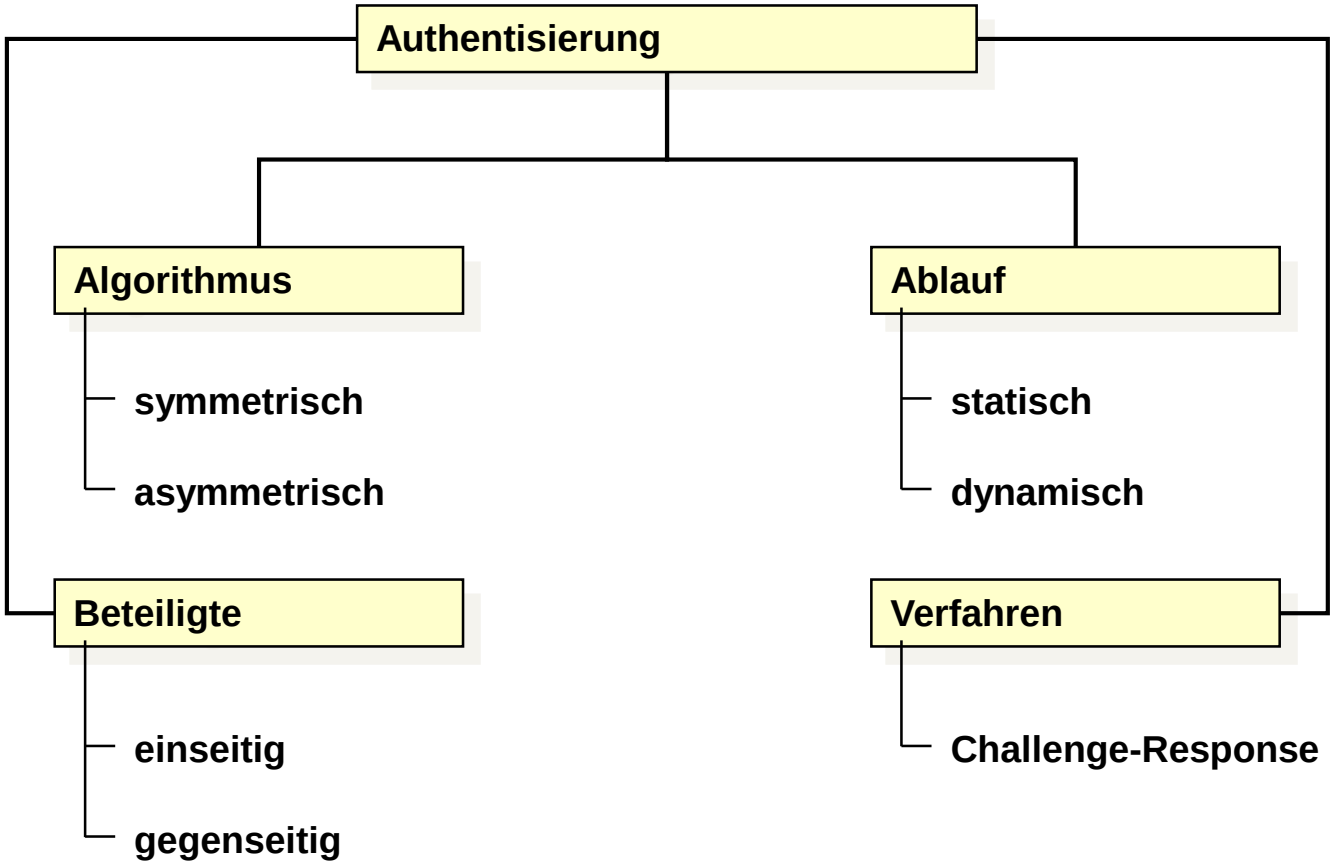
Einschub Chipkarte: Kommunikationsmodell



Einschub Chipkarte: Chipkarten-Protokoll

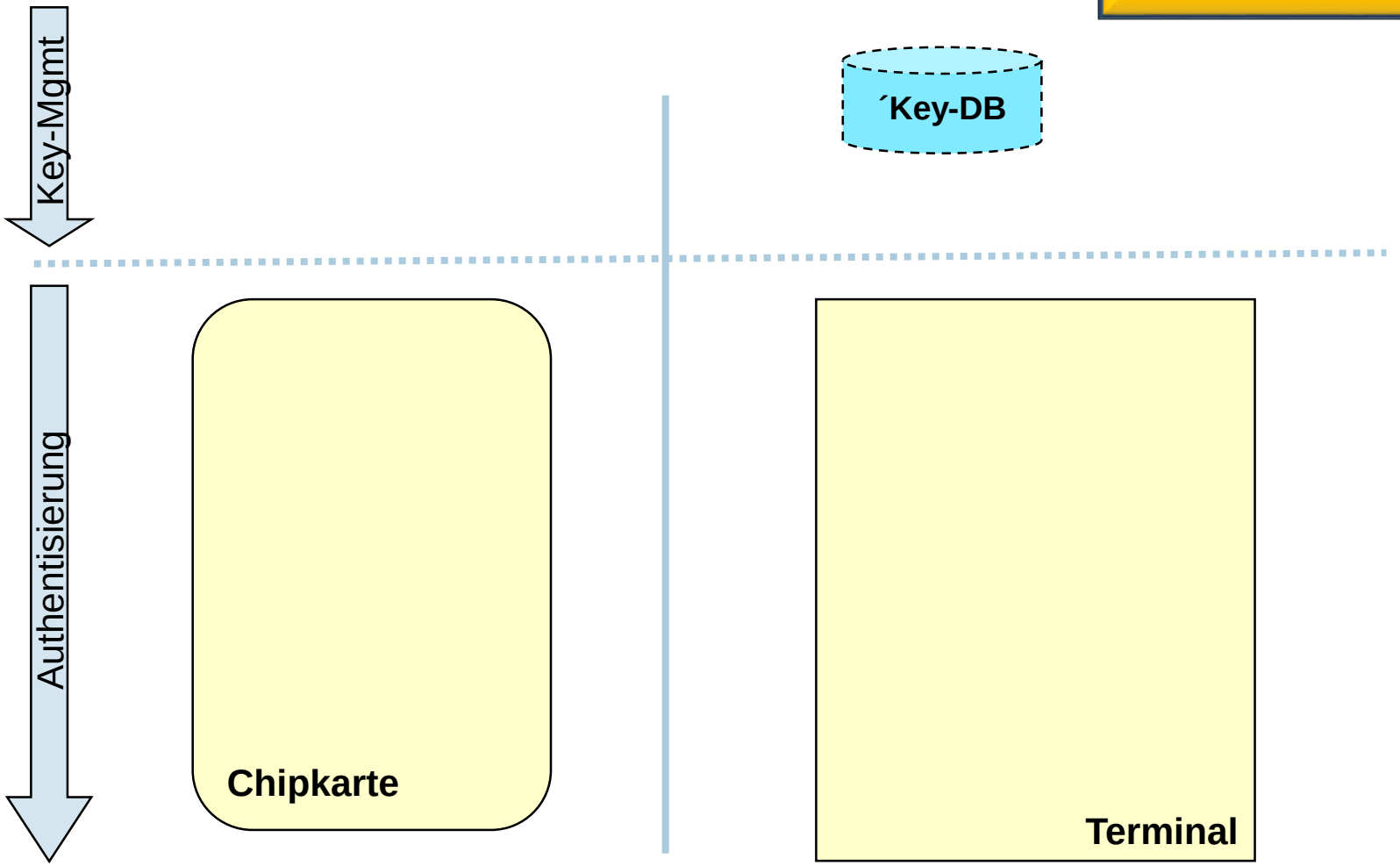


Klassifikationsschema Authentisierung (nach Rankl/Effing)

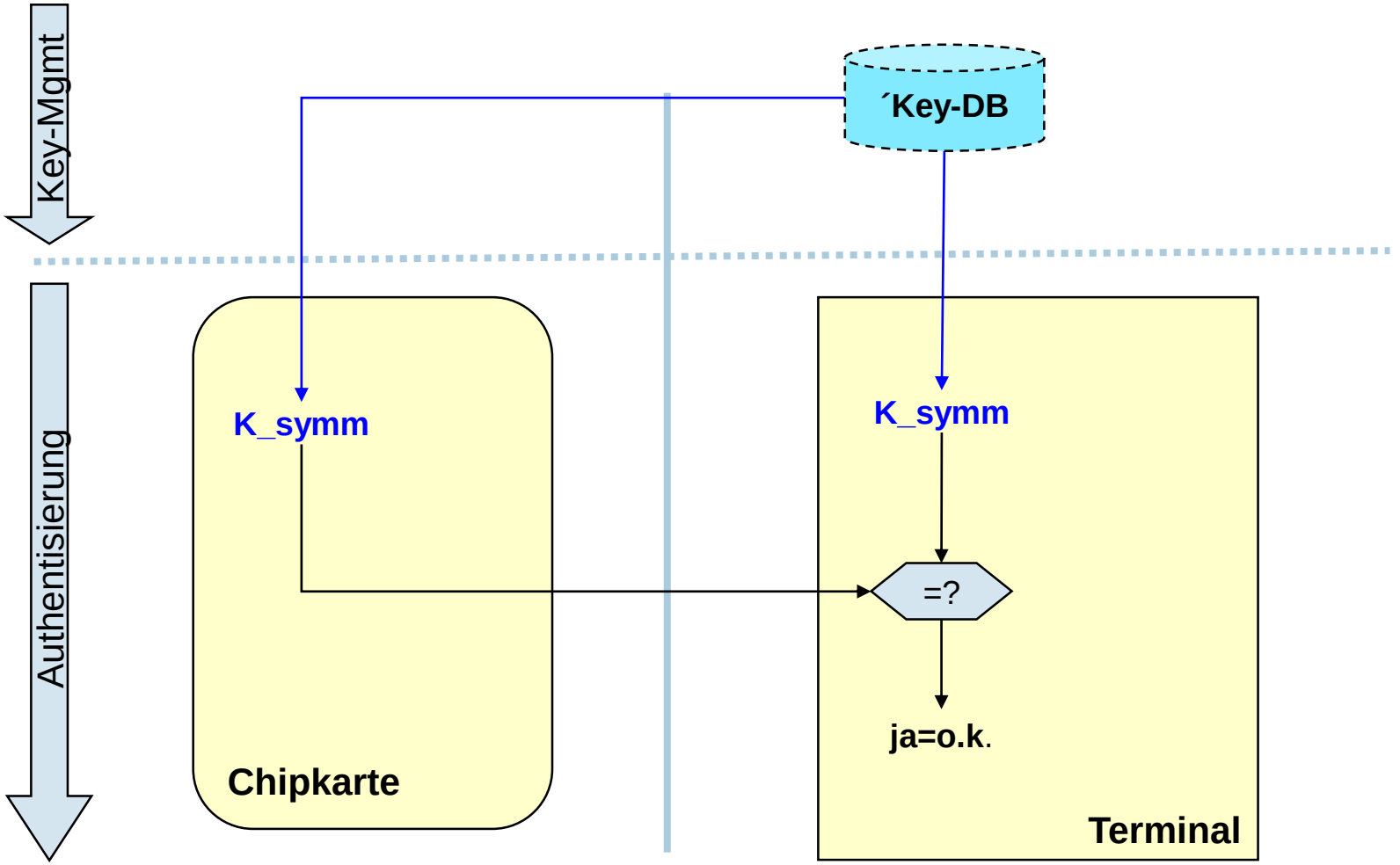


K_symm

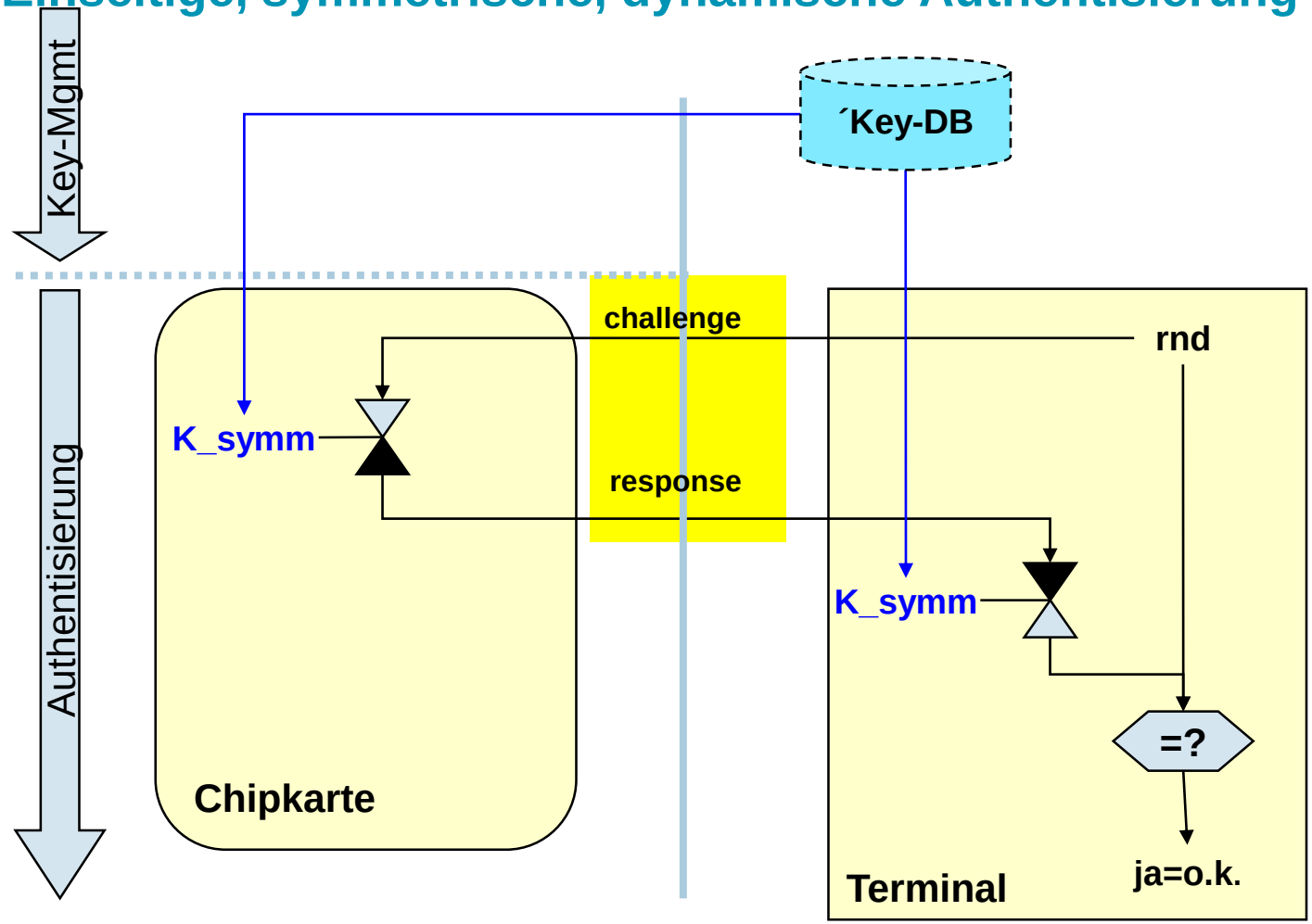
Grundschema für Authentisierungsverfahren



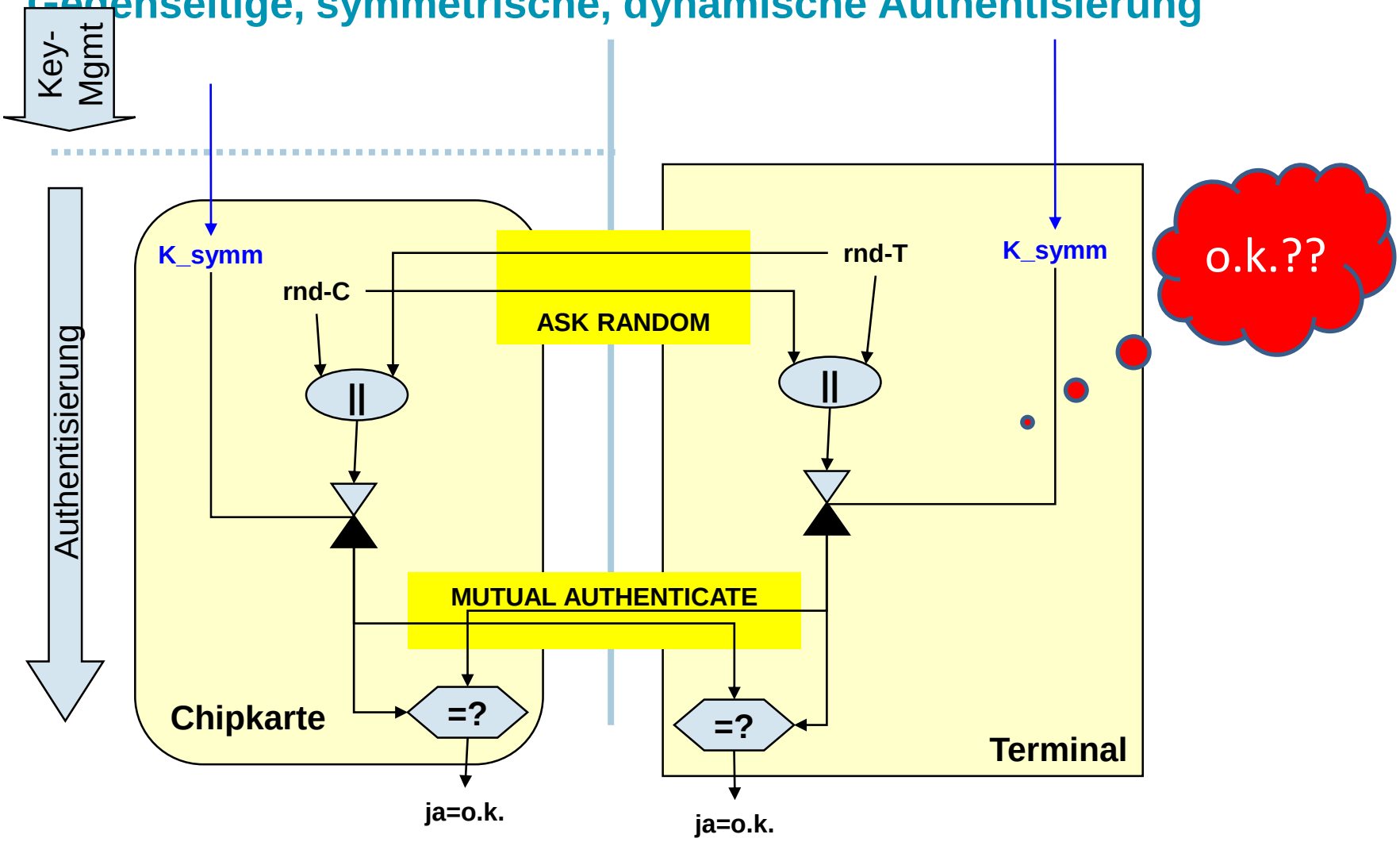
Einseitige, statische, symmetrische Authentisierung



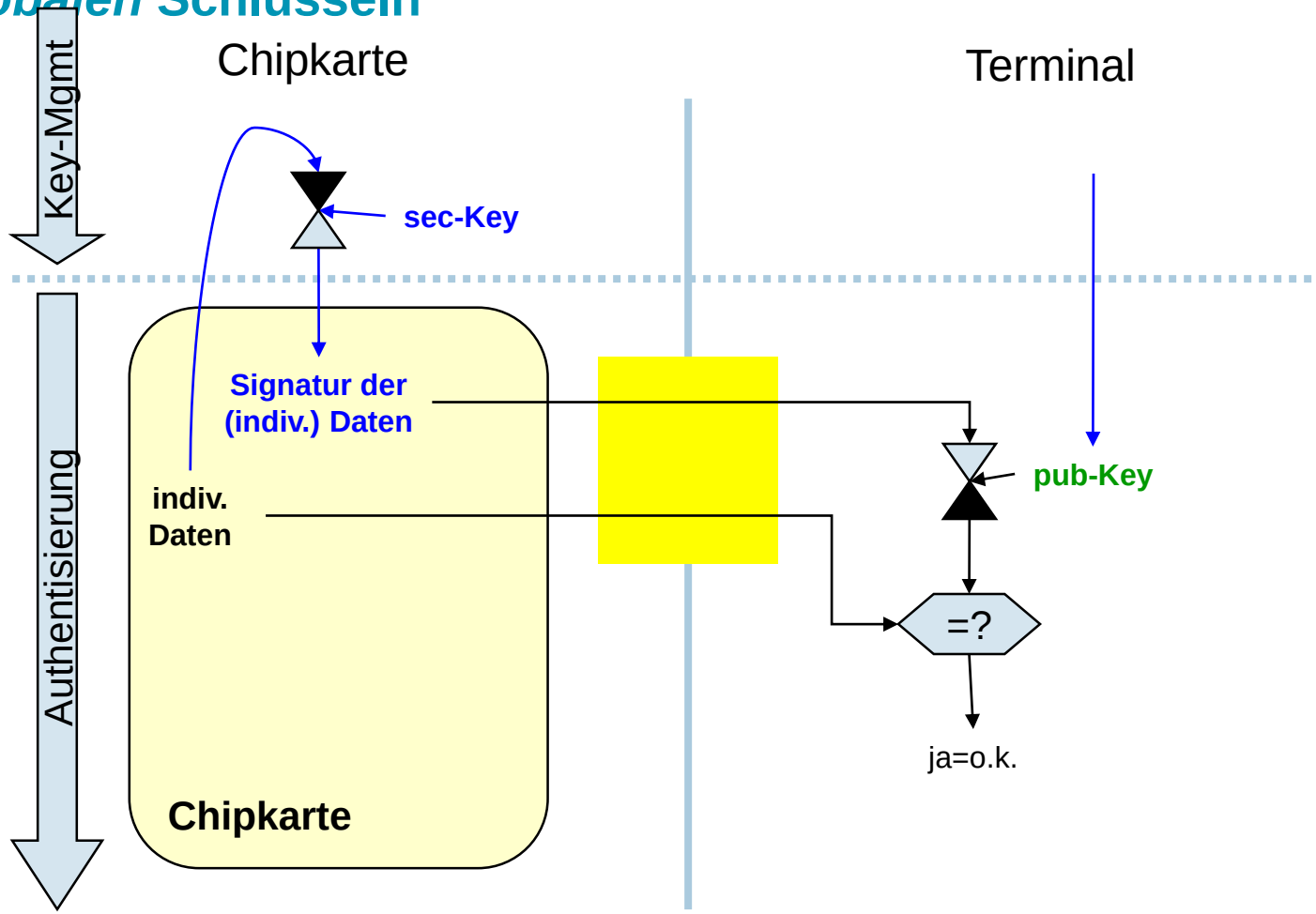
Einseitige, symmetrische, dynamische Authentisierung



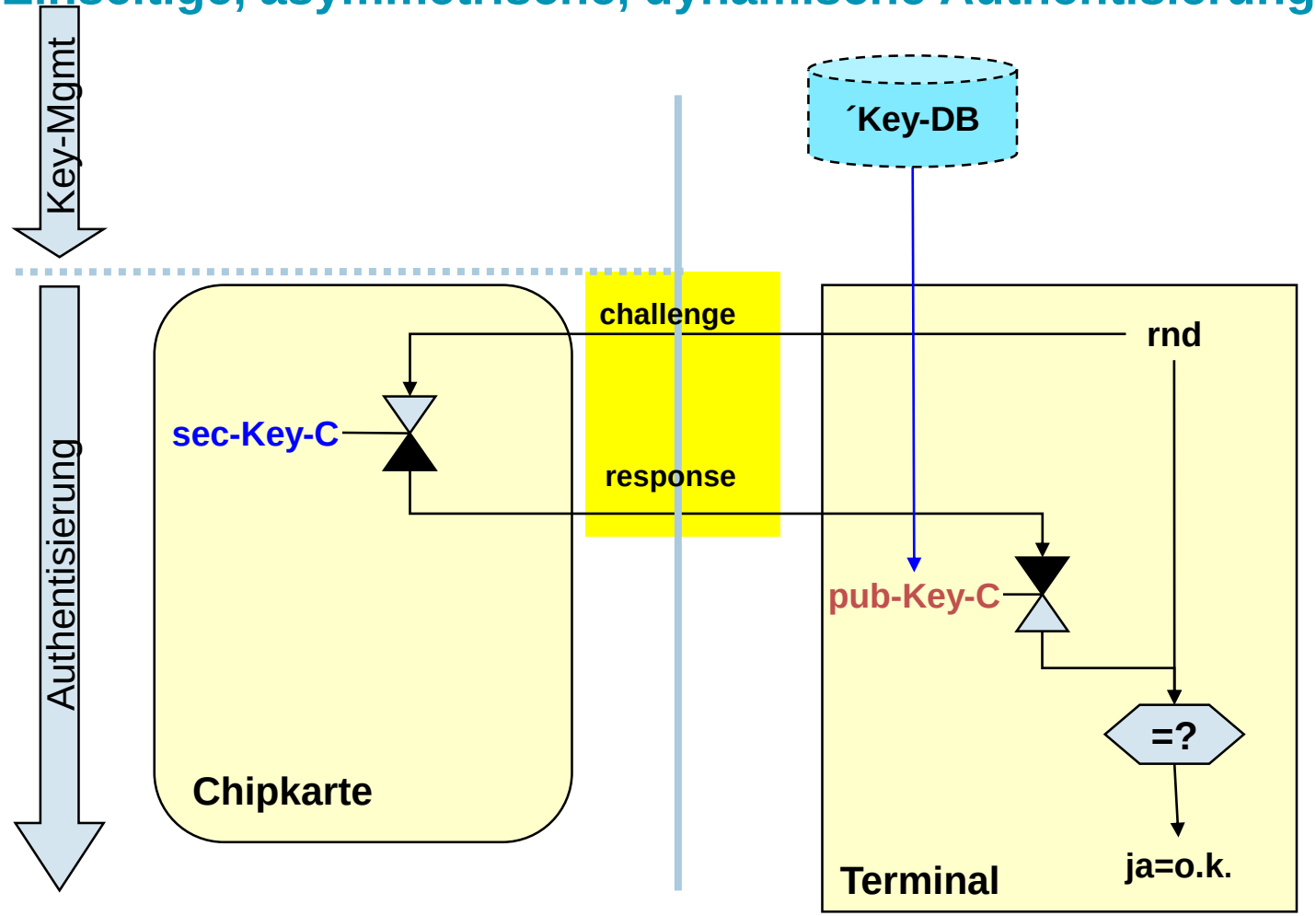
Gegenseitige, symmetrische, dynamische Authentisierung



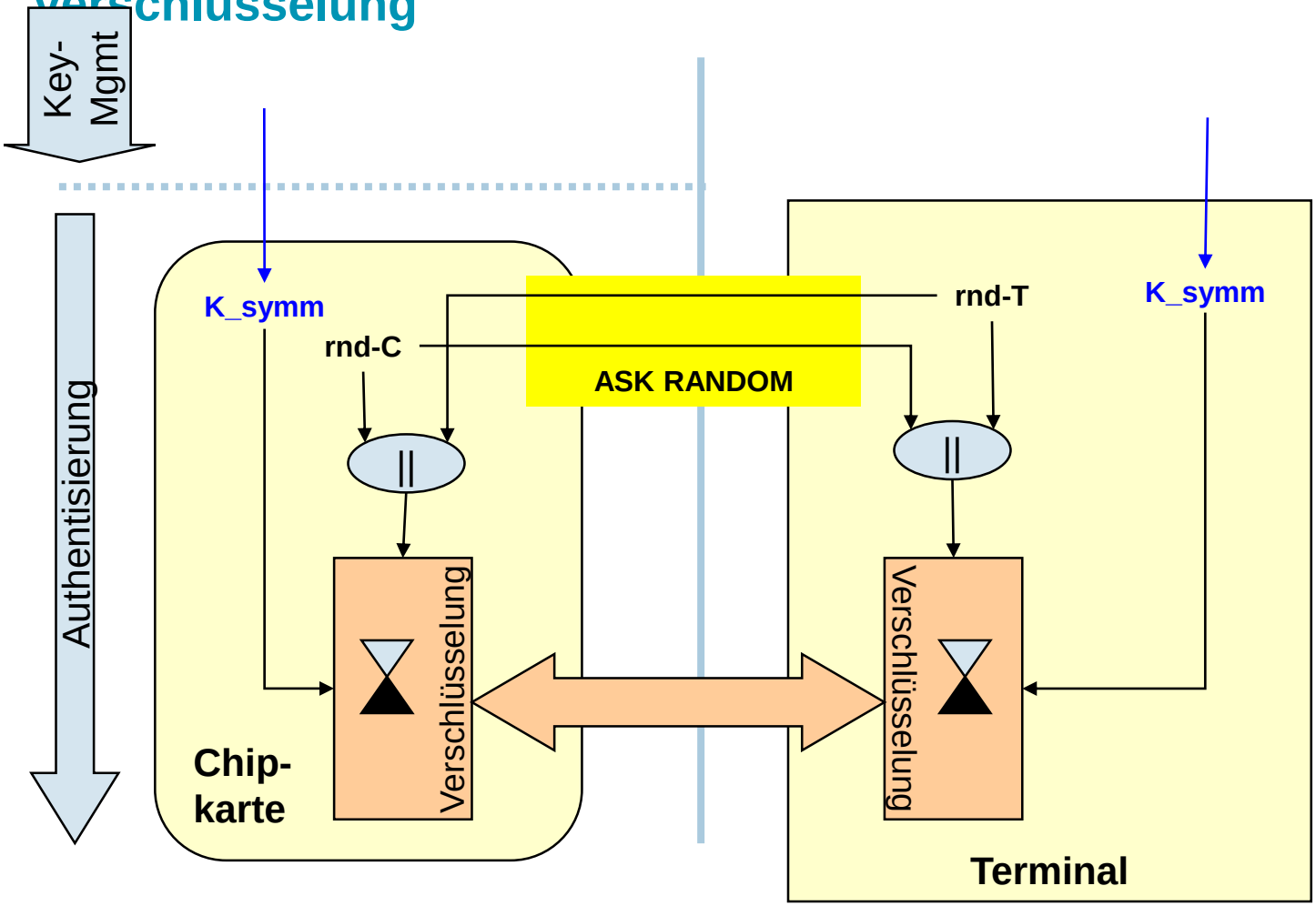
Einseitige, statische, asymmetrische Authentisierung mit *globalen* Schlüsseln



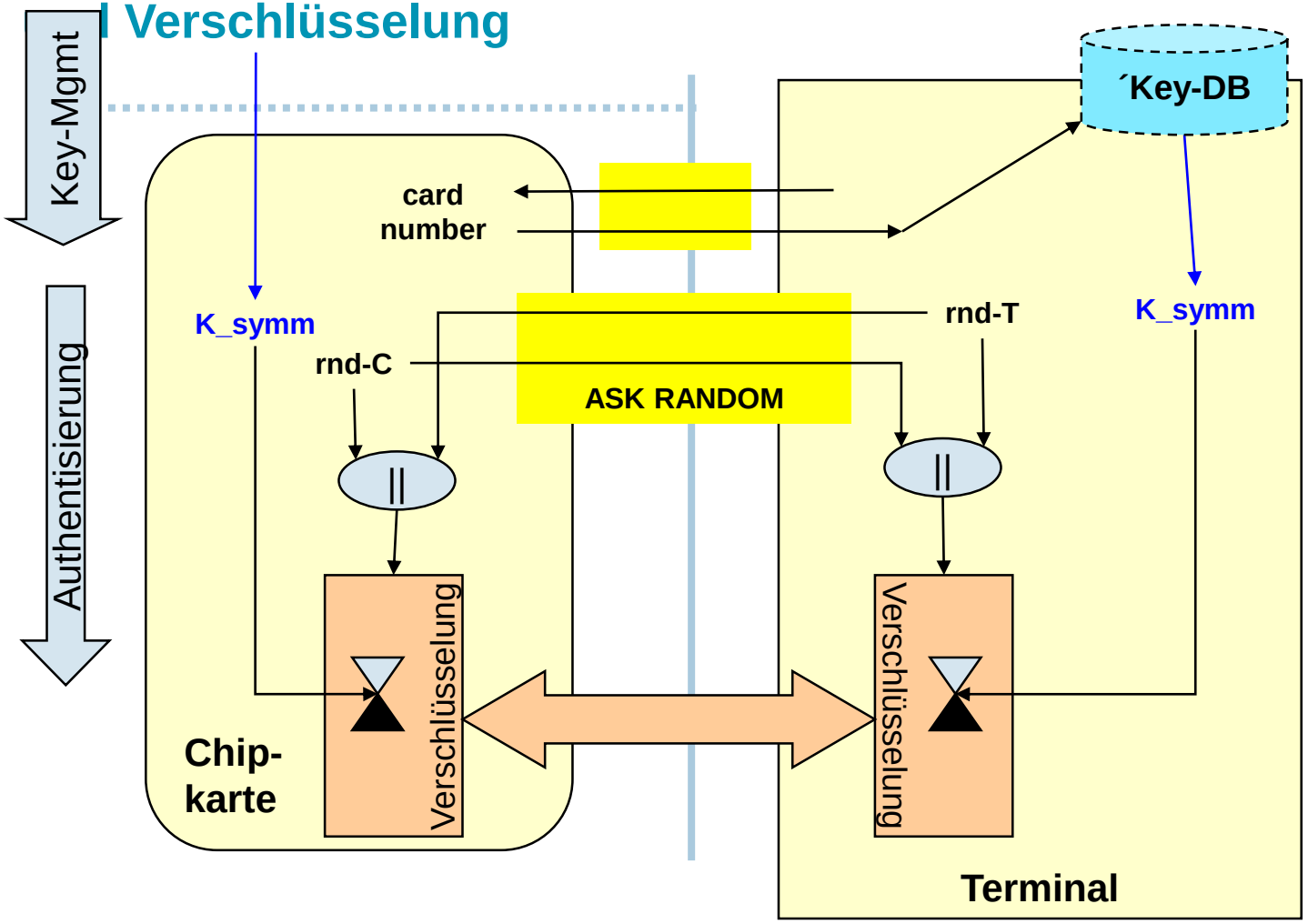
Einseitige, asymmetrische, dynamische Authentisierung



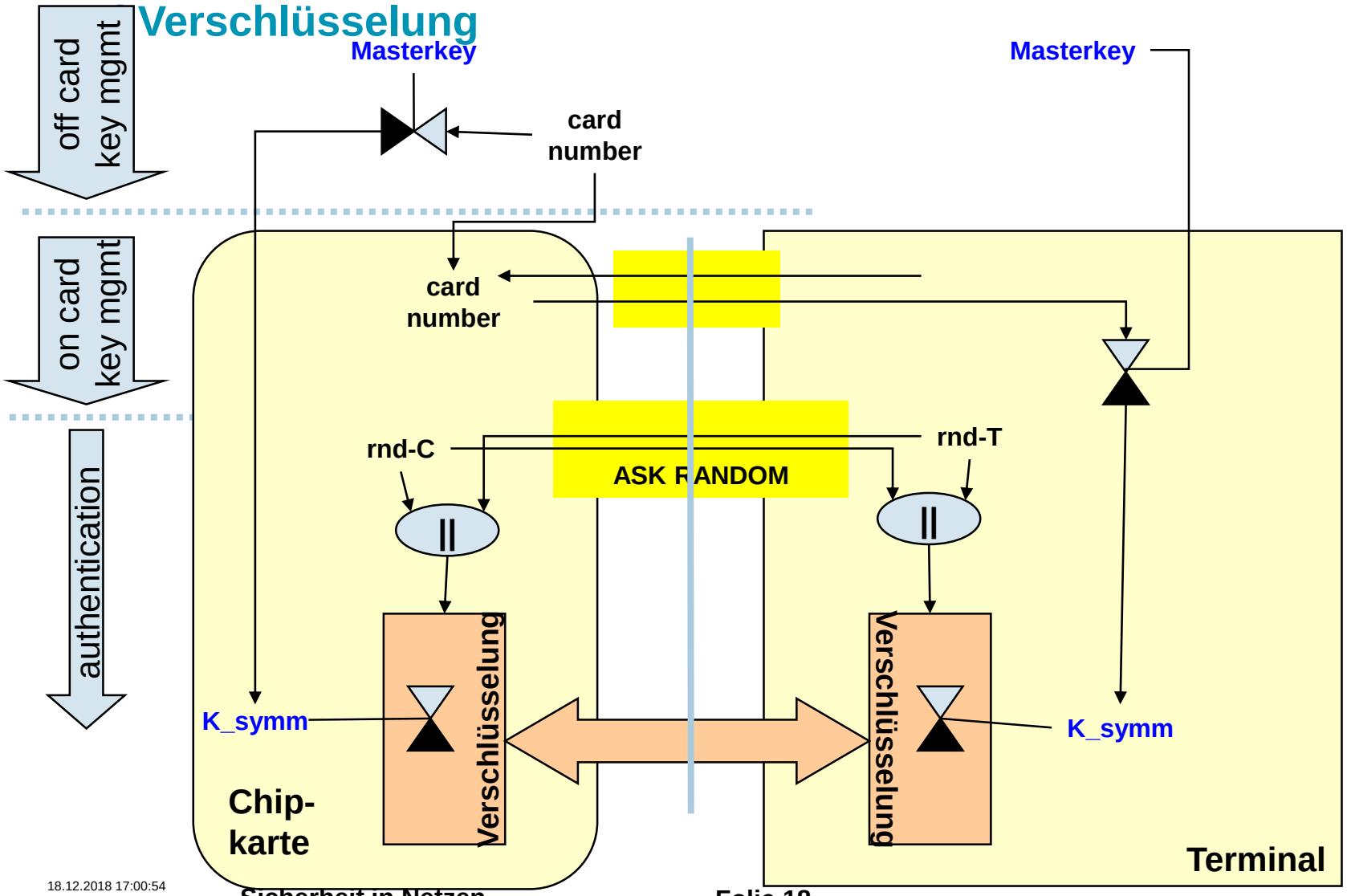
Gegenseitige, symmetrische, dynamische Authentisierung und Verschlüsselung



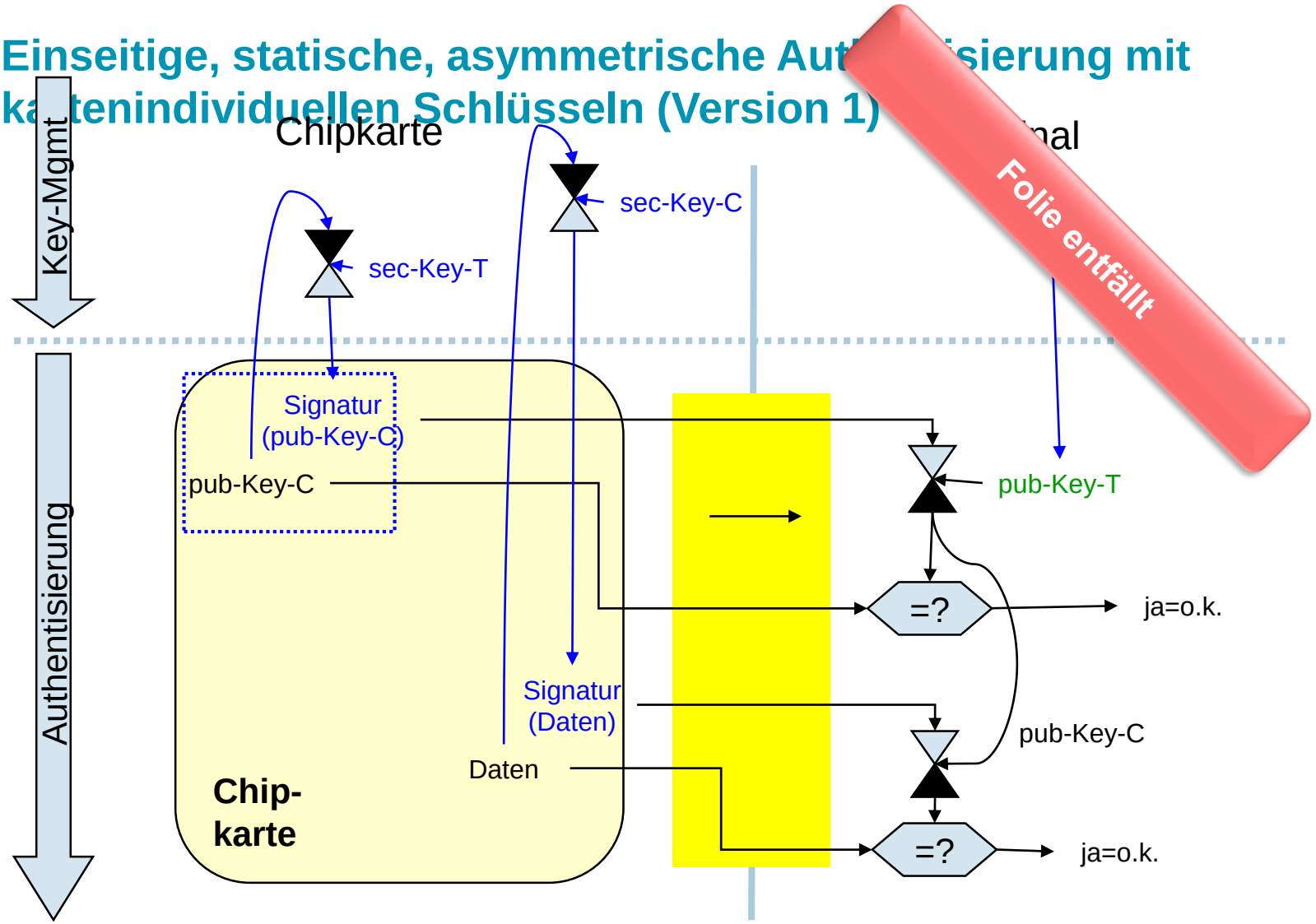
Gegenseitige, symm., dynam., Authentisierung mit Key-Mgmt und Verschlüsselung



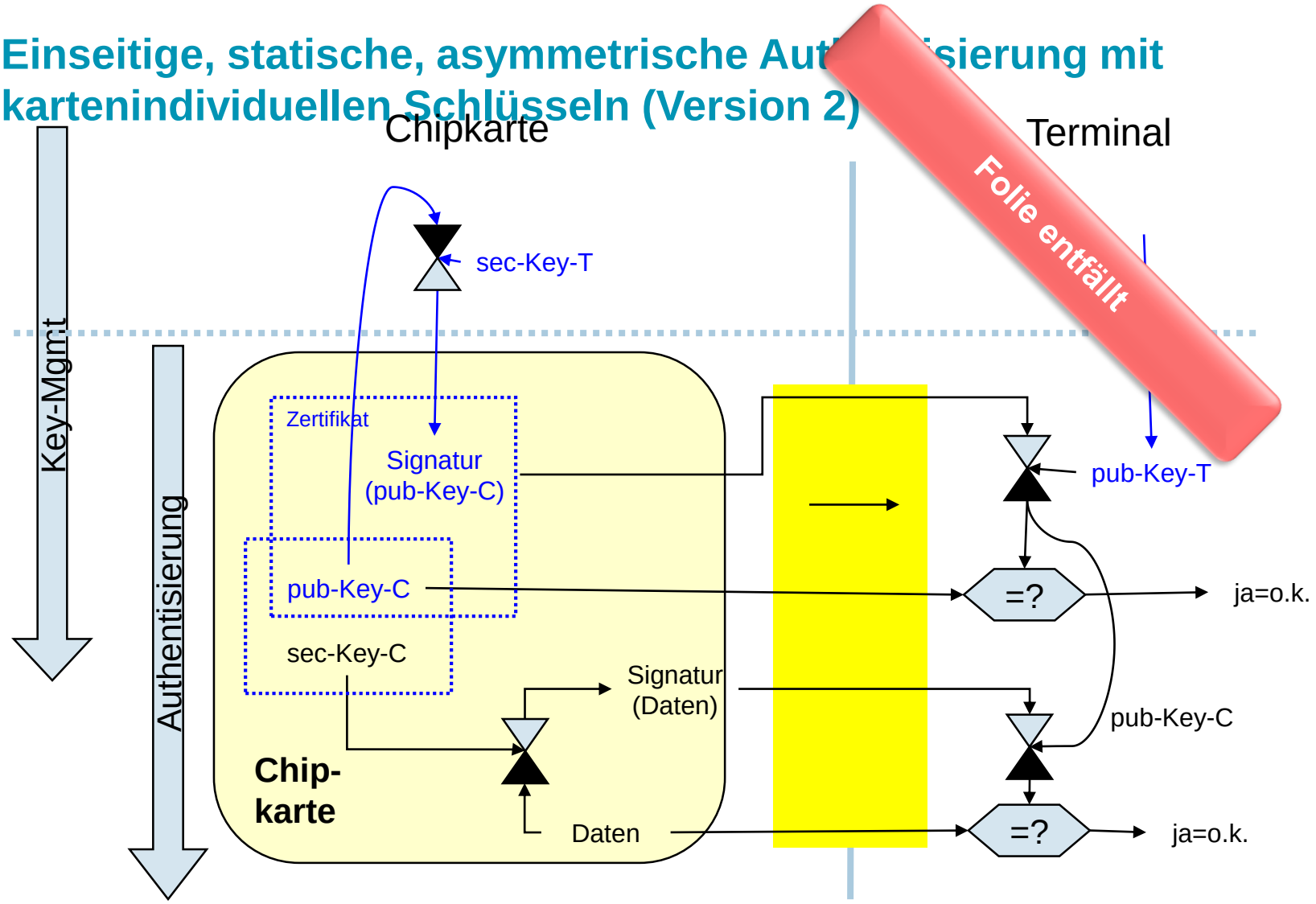
Gegenseitige, dynam., symm. Authentisierung mit Master-Key Verschlüsselung



Einseitige, statische, asymmetrische Authentisierung mit kartenindividuellen Schlüsseln (Version 1)



Einseitige, statische, asymmetrische Authentisierung mit kartenindividuellen Schlüsseln (Version 2)



einseitige, statische, asymmetrische Authentisierung mit kartenindividuellen Schlüsseln und teilweisem oncard-Key-Mmgt