Security-Managementsystem für verteilte Messgeräte

2. SELMA Workshop
15.-16. Oktober 2003,
Berlin

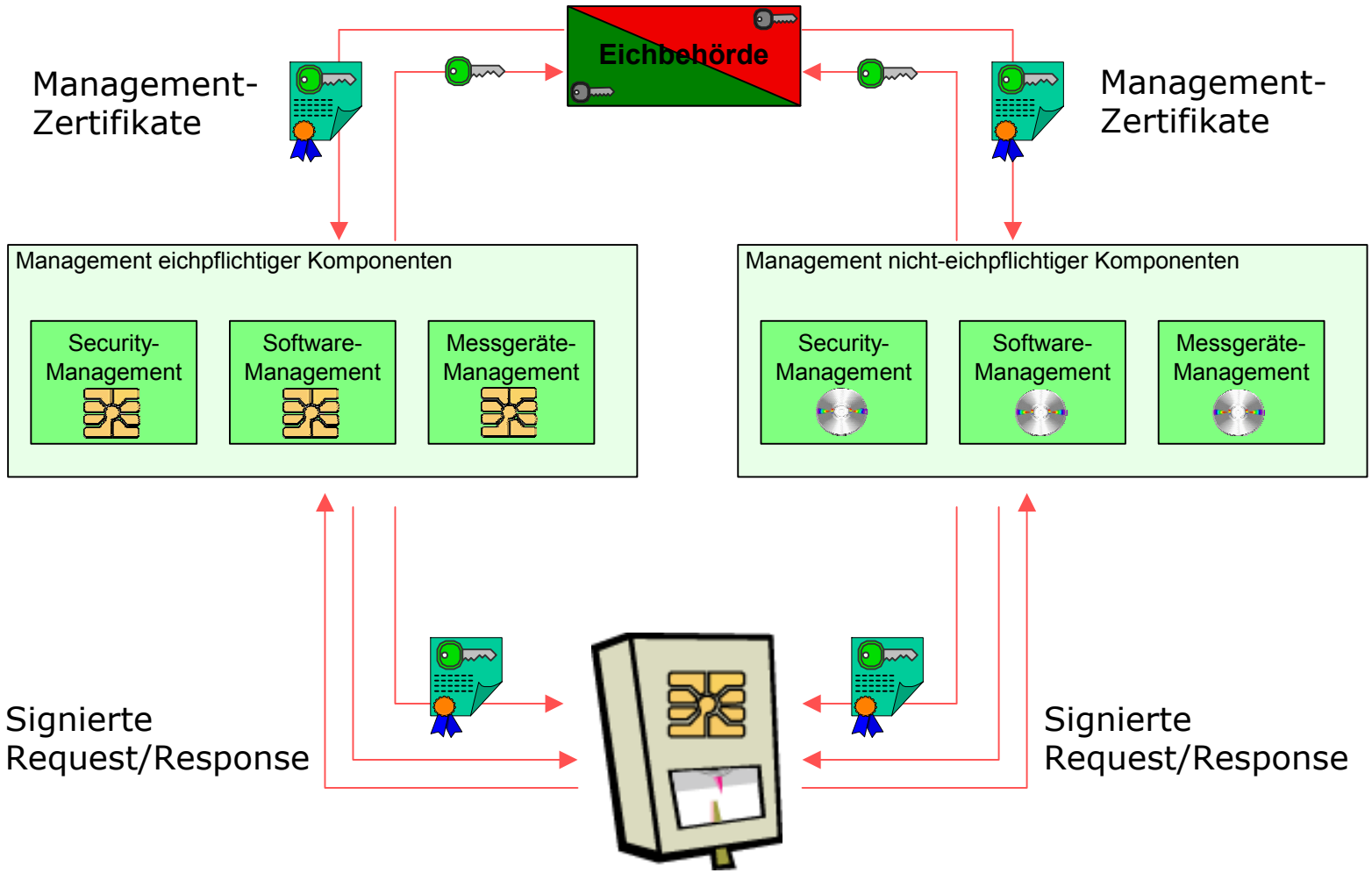
Luigi Lo Iacono

Institut für Digitale Kommunikationssysteme,
Universität Siegen

Agenda

- SELMA Managementsysteme
- SELMA Security-Managementsysteme
- Schematischer Aufbau/Funktionsweise
- Zusammenfassung

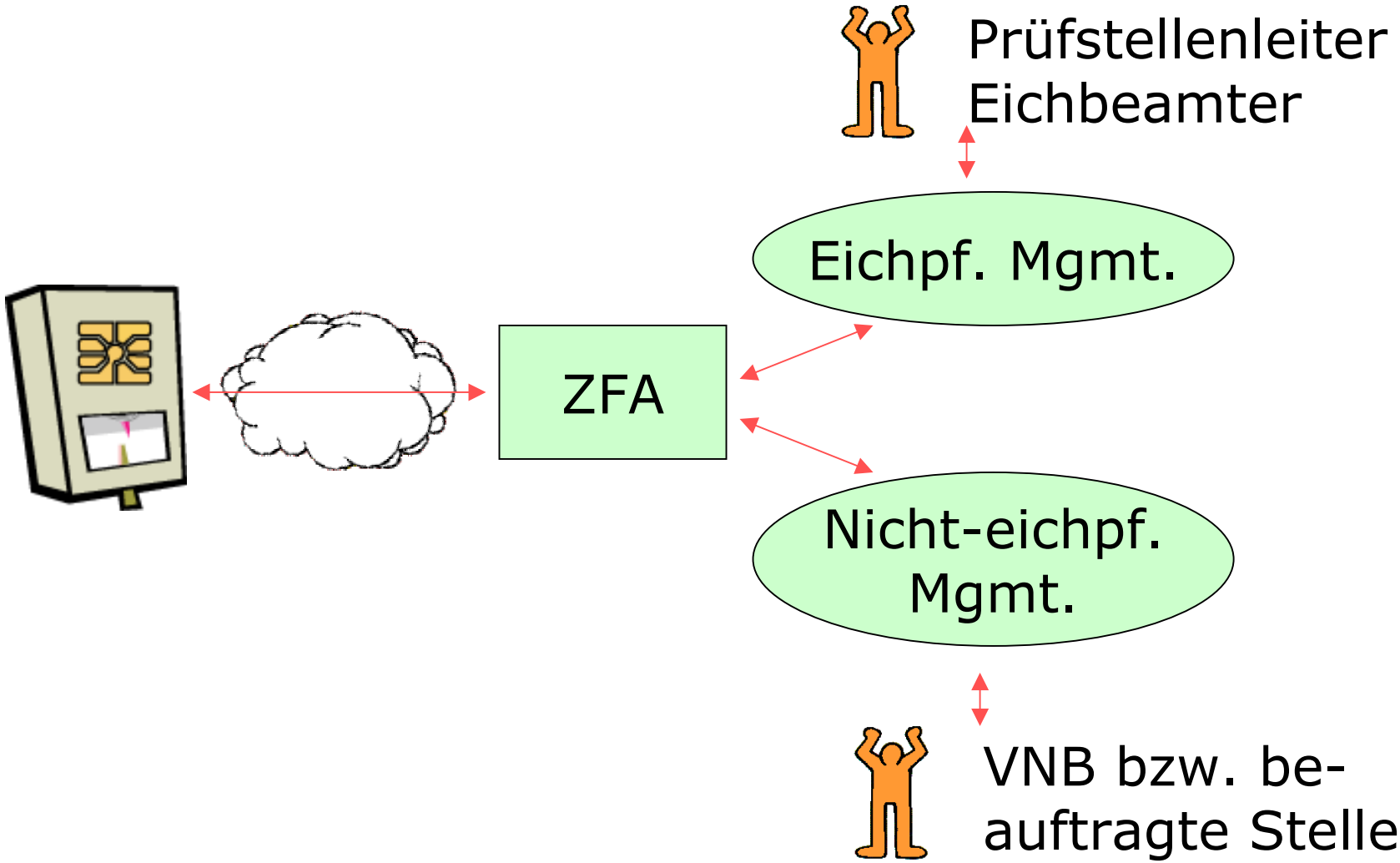
SELMA Managementsysteme



SELMA Security-Managementsysteme

- Eichpflichtig
  - Schlüsselmanagement (MG, AGME, PTB, Prüfstellen)
  - Logbuchverwaltung
  - Uhrzeit stellen
  - Verarbeitung/Auswertung von Alarmen
- Nicht eichpflichtig
  - Schlüsselmanagement (VNB, Lieferant, DAS)
  - Logbuchverwaltung
  - Uhrzeit setzen

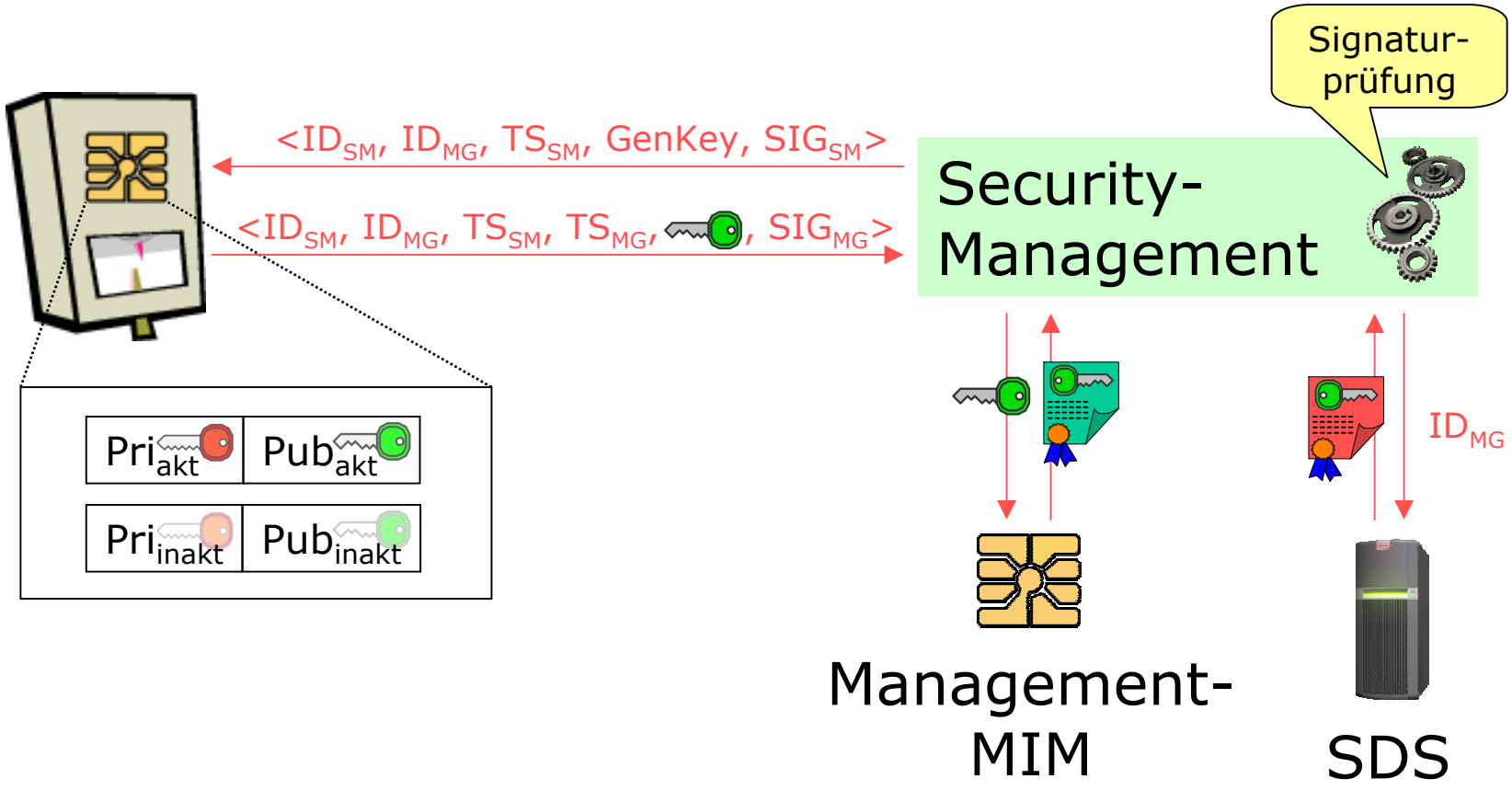
SELMA Security-Managementsysteme II



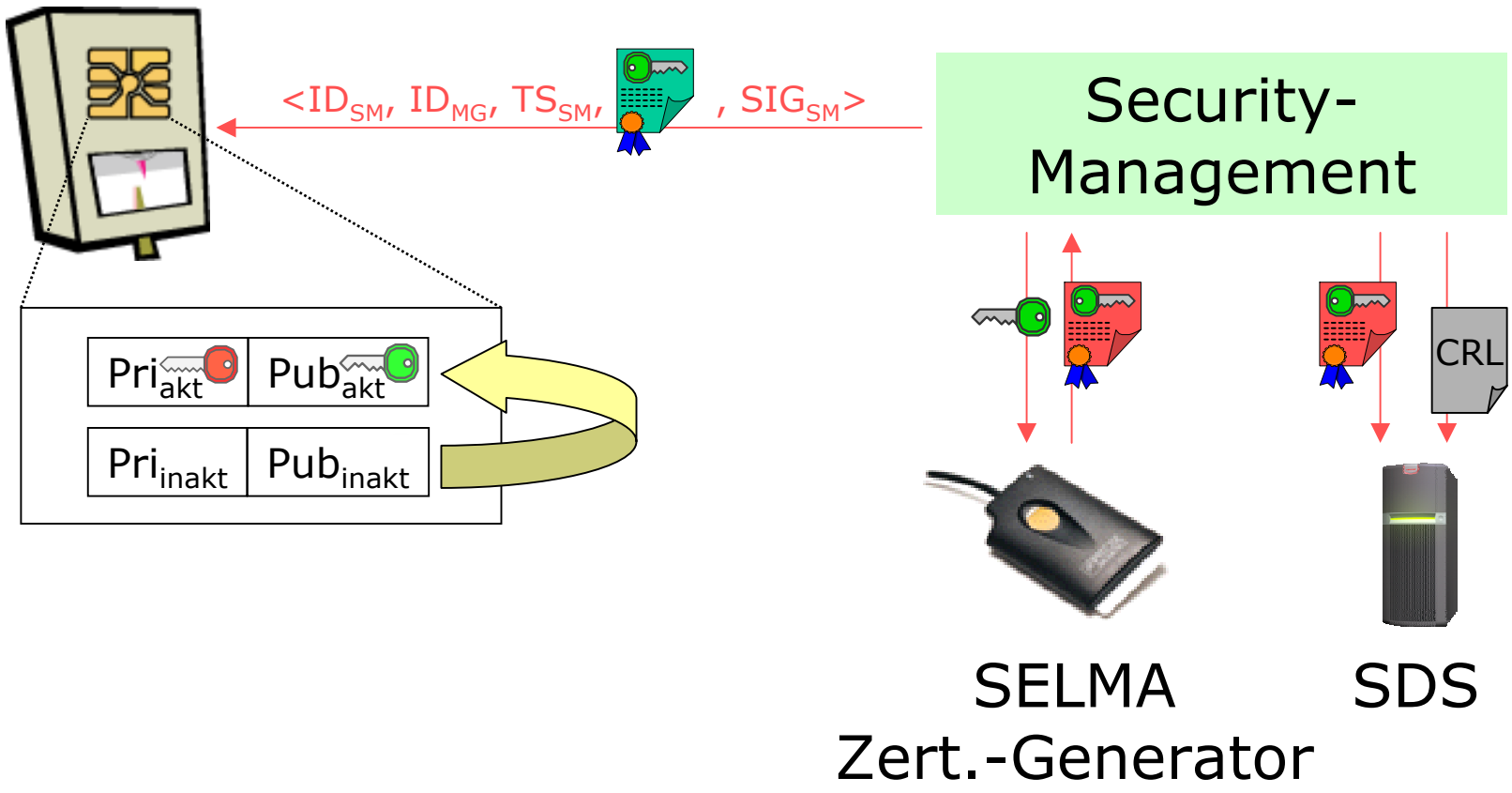
Schlüsselmanagement

- Schlüsselpaar-Erzeugung
- Zertifikats-Erzeugung
- SDS
  - Verwaltung der Zertifikate
  - Verwaltung der CRL
- Signaturschlüsselwechsel
- Verwaltung der öffentlichen Prüfschlüssel in den Messgeräten
  - Übertragung über offene Netze nur als Zertifikat
  - Löschen durch signierte Kommandos

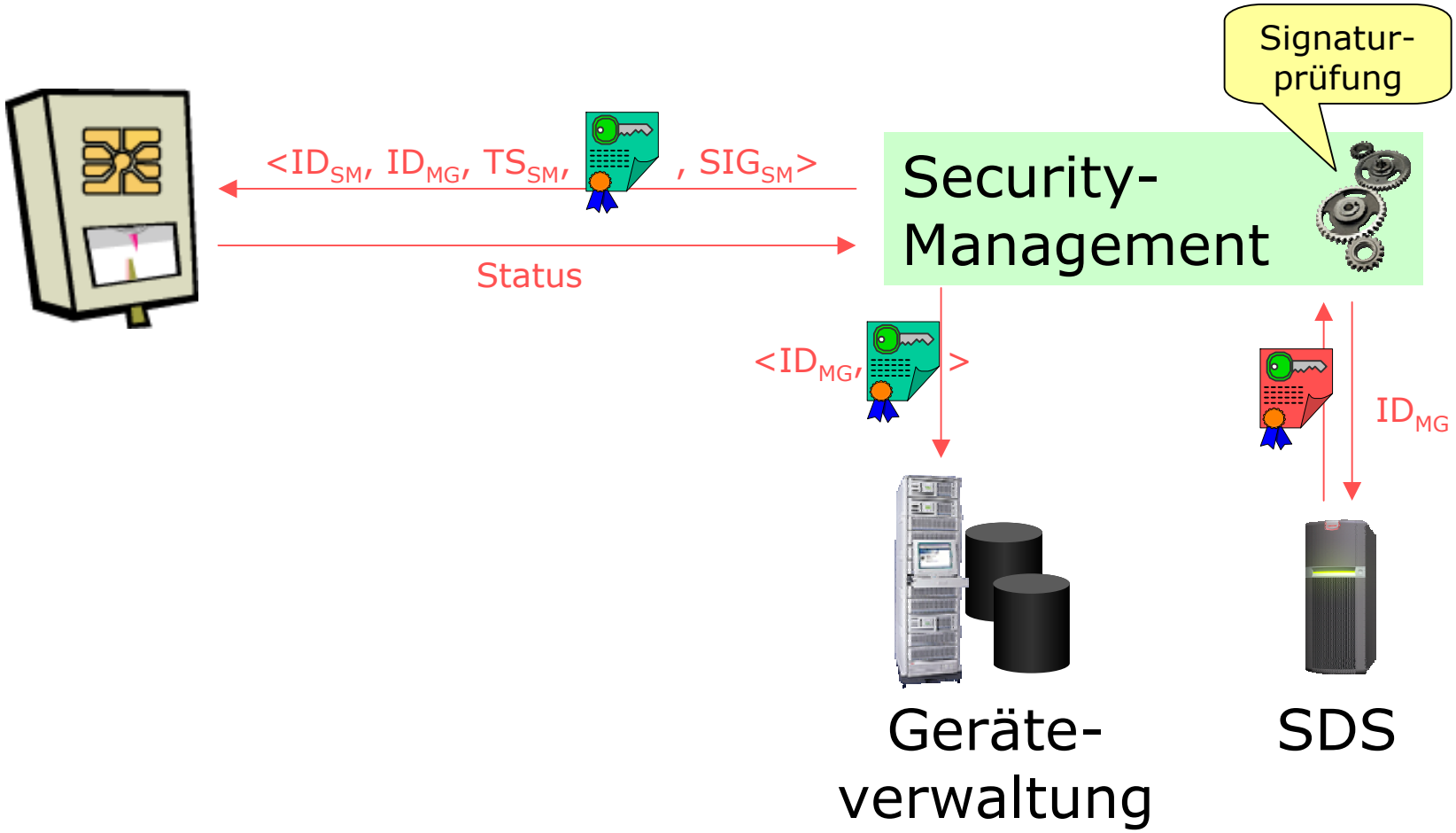
Schlüsselmanagement – Signaturschlüsselwechsel



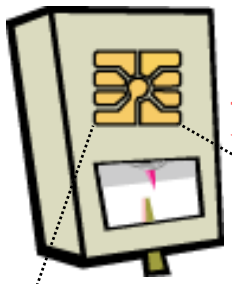
Schlüsselmanagement – Signaturschlüsselwechsel II

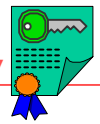


Schlüsselmanagement – Laden öffentlicher Schlüssel



Schlüsselmanagement – Beispiel: Teilnetzveräußerung I

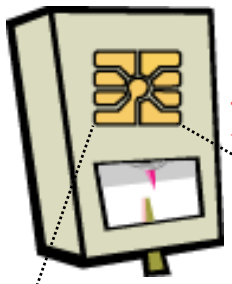


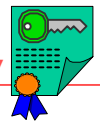
<ID_{SM}, ID_{MG}, TS_{SM}, (DEL,  ,3), SIG_{SM}>

Security-Management

0	AGME	1
1	AGME	0
2	PTB	0,1
3		0,1
4	Prüfstelle	0,1
5	VNB1	3,4

Schlüsselmanagement – Beispiel: Teilnetzveräußerung II

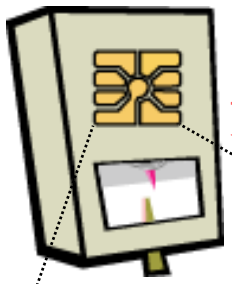


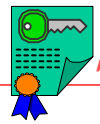
<ID_{SM}, ID_{MG}, TS_{SM}, (DEL,  ,4), SIG_{SM}>

Security-Management

0	AGME	1
1	AGME	0
2	PTB	0,1
3		0,1
4		0,1
5	VNB1	3,4

Schlüsselmanagement – Beispiel: Teilnetzveräußerung III

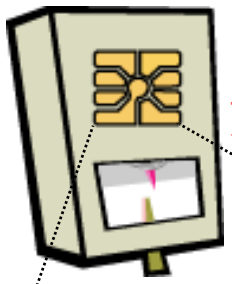


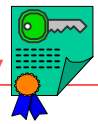
<ID_{SM}, ID_{MG}, TS_{SM}, (INS,  ,3), SIG_{SM}>

Security-Management

0	AGME	1
1	AGME	0
2	PTB	0,1
3	Prüfstelle	0,1
4		0,1
5	VNB1	3,4

Schlüsselmanagement – Beispiel: Teilnetzveräußerung IV

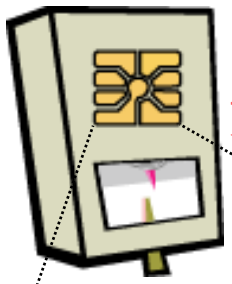


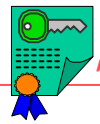
<ID_{SM}, ID_{MG}, TS_{SM}, (DEL,  ,5), SIG_{SM}>

Security-Management

0	AGME	1
1	AGME	0
2	PTB	0,1
3	Prüfstelle	0,1
4		0,1
5		3,4

Schlüsselmanagement – Beispiel: Teilnetzveräußerung V

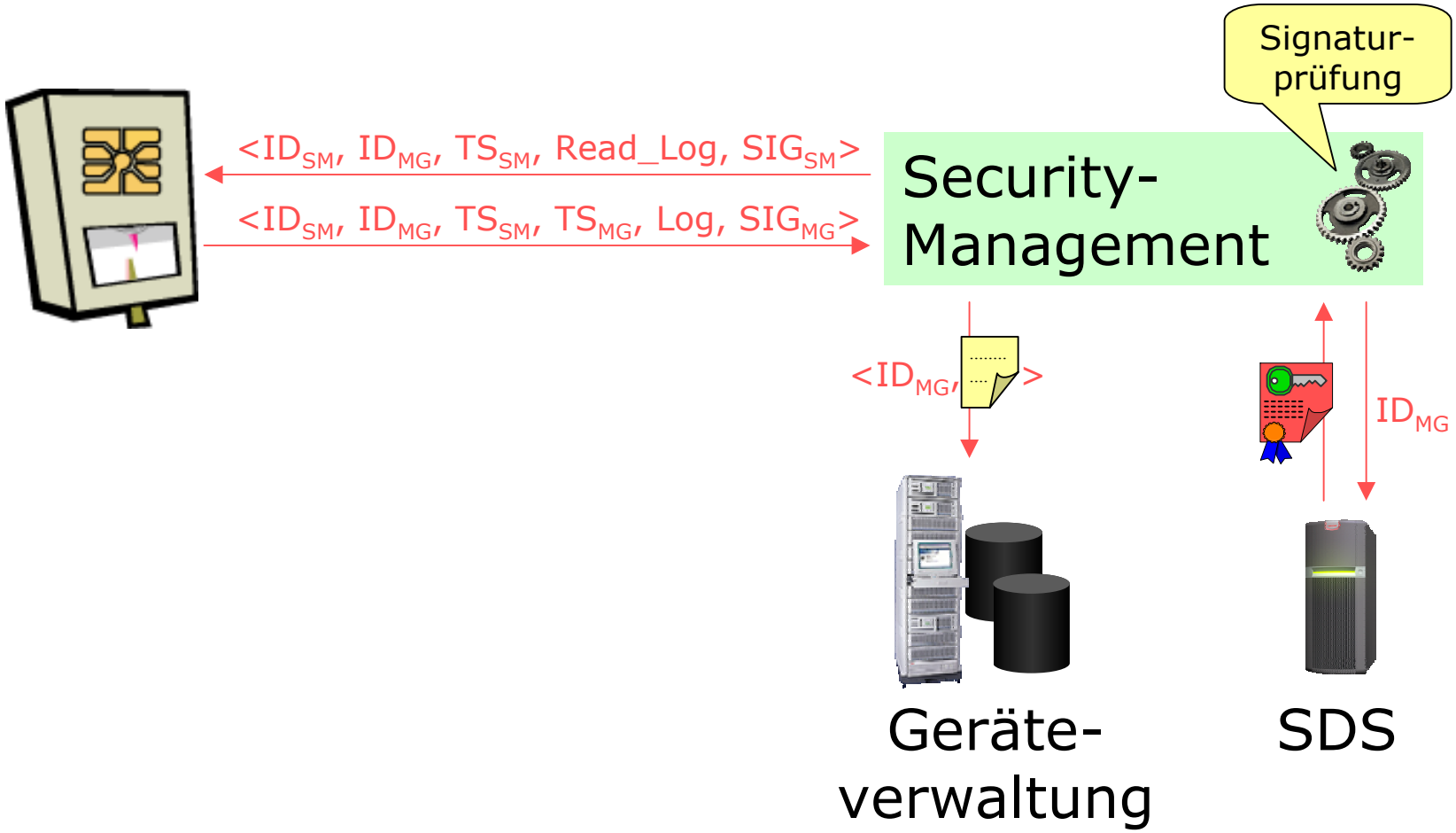


<ID_{SM}, ID_{MG}, TS_{SM}, (INS,  ,5), SIG_{SM}>

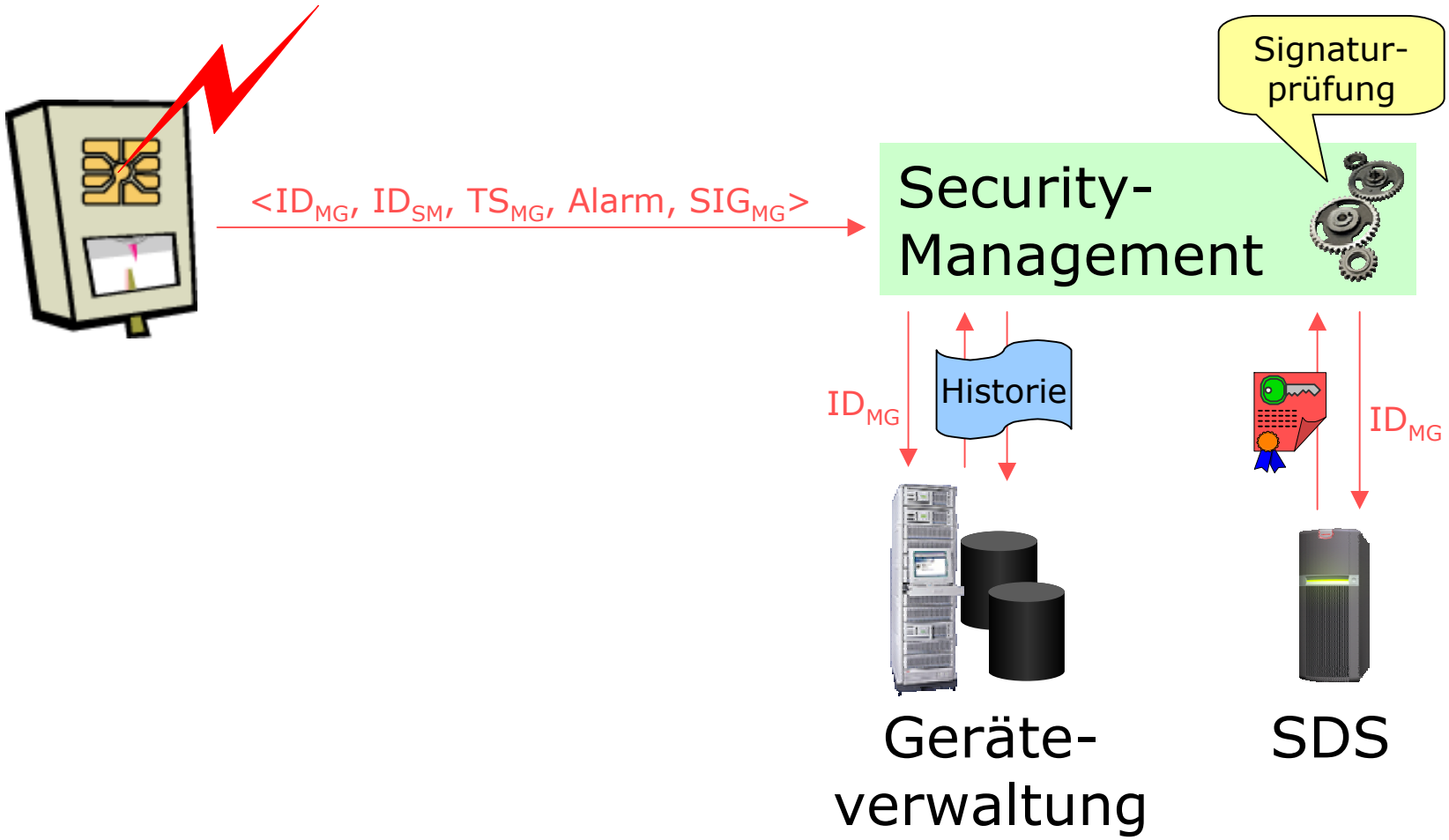
Security-Management

0	AGME	1
1	AGME	0
2	PTB	0,1
3	Prüfstelle	0,1
4		0,1
5	VNB2	3,4

Logbuchverwaltung



Alarme


<ID_MG, ID_SM, TS_MG, Alarm, SIG_MG>
Signatur-
prüfung
Security-
Management
ID_MG
Historie
ID_MG
Geräte-
verwaltung
SDS

Zusammenfassung

- Die SELMA-Messgeräte enthalten eine Signaturerstellungseinheit
- Die Authentikation von Management-Zugriffen erfolgt über digitale Signaturen
- Zur Verwaltung der kryptographischen Systemparameter müssen entsprechende Managementsysteme zur Verfügung stehen
- Es muss zwischen eichpflichtigem und nicht-eichpflichtigen Management unterschieden werden


Fragen