Das Ende der E-Mail – Technologien für die Marktkommunikation

Würzburg – 15.11.2018

robotron®

Hauptpunkte

- Die E-Mail ist tot, es lebe der Webservice?
- Sicherheitsanforderungen
- Zwei Vorschläge des BDEW
  - AS4 nach dem Vorbild der ENTSOG
  - Smart Metering Public Key Infrastructure nach dem Vorbild des BSI
- Das Ende der E-Mail ist nicht das Ende von EDIFACT.

robotron®

Agenda

1	E-Mail und die Sicherheitsanforderungen
2	Alternative Technologien
3	BDEW-Position
4	Nächste Schritte

Ist die E-Mail noch zeitgemäß?

- E-Mail als bewährte Technologie
  - gehärtete Prozesse
  - preiswerte Verarbeitung
- steigende Anforderungen
  - Verkürzung der Fristen
  - Datenschutz und Datensicherheit
  - Automatisierung
  - Effizienz
  - Transaktionssicherheit
  - Einbindung in europäische Leitplanken

=> Latenzzeit der Kommunikation muss reduziert werden

Vergleich E-Mail Webservice

	E-Mail	Webservice
Kommunikation	asynchron	synchron
Nichtabstreitbarkeit	CONTRL	synchrone Antwort
Umsetzung	bereits vorhanden	mit Aufwand verbunden
Geschwindigkeit	bis zu 6h Verzögerung	schnell
Datenschutz und Datensicherheit	Inhaltverschlüsselung Signierung	Inhaltsverschlüsselung Transportverschlüsselung Signierung

Sicherheitsanforderungen

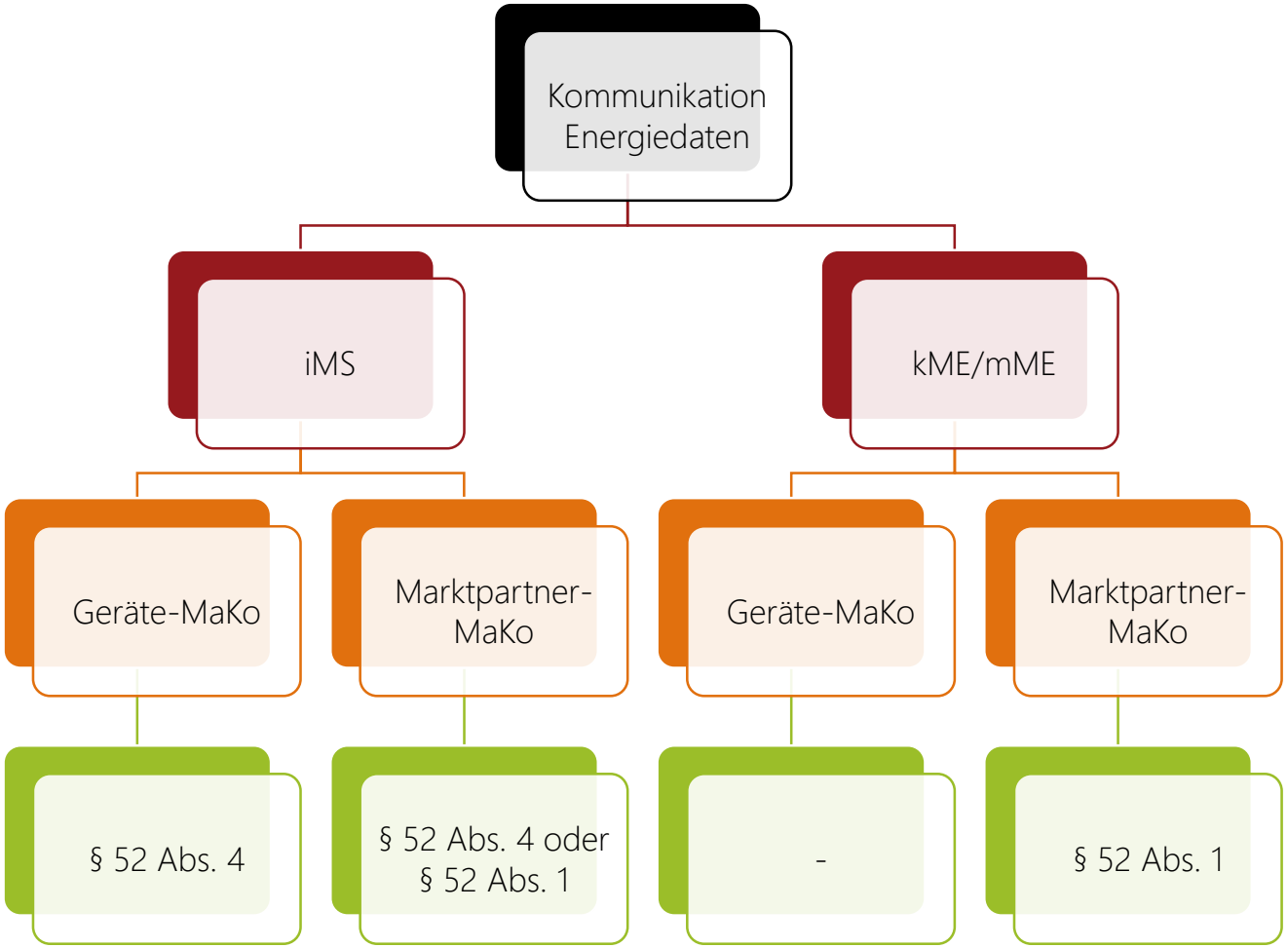
MsbG

- § 52 Abs. 1 MsbG
  - Die [...] berechtigten Stellen haben eine verschlüsselte elektronische Kommunikation von personenbezogenen Daten, von Mess-, Netzzustands- und Stammdaten in einem einheitlichen Format zu ermöglichen, die den Bestimmungen dieses Gesetzes genügt. [...]
- § 52 Abs. 4 MsbG
  - Aus intelligenten Messsystemen stammende personenbezogene Daten, Stammdaten und Netzzustandsdaten dürfen nur zwischen Teilnehmern an der Smart-Metering-Public-Key-Infrastruktur des Bundesamtes für Sicherheit in der Informationstechnik kommuniziert werden [...]
- § 75 Nr. 1 MsbG
  - [...] kann die Bundesnetzagentur Festlegungen nach § 29 Absatz 1 des Energiewirtschaftsgesetzes treffen im Sinne von § 52 zur Gewährleistung eines einheitlichen Sicherheitsstandards für die nicht unmittelbare Kommunikation mit dem intelligenten Messsystem im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik

Unterscheidung Marktkommunikation nach BDEW

- Geräte-Marktkommunikation
  - Kommunikation mit kME oder mME und einem Marktpartner
  - Kommunikation zw. SMGW und EMT (Marktpartner)
    - Nur hier gilt § 52 Abs. 4 MsbG
    - BSI TR-03116 Teil 3: Intelligente Messsysteme
    - Smart-Metering-Public-Key-Infrastruktur
    - Hardwaresicherheitsmodul für die Speicherung der Zertifikate
- Marktpartner-Marktkommunikation
  - Kommunikation zwischen Marktpartnern
  - BSI TR-03116 Teil 4: Kommunikationsverfahren in Anwendungen
  - Anwendung aus dem aktuellen Signatur/Verschlüsselungsverfahren für EDIFACT-E-Mail-Kommunikation bekannt

Sicherheitsanforderungen des MsbG



robotron®

BSI TR-03116 Teil 3

für § 52 Abs. 4

- WebService mit TLS-Protokoll
  - verschlüsselter/integritätsgesicherter und gegenseitig authentisierter Kanal
  - Cipher-Suites
  - Signaturalgorithmen
  - Vorgaben für die Zertifikate
  - Regeln für den Sperrlistenabgleich
- Inhaltsdatenverschlüsselung
  - Verschlüsselungs- und Signaturverfahren
- Smart Metering Public Key Infrastruktur (SM-PKI)
  - eine Root-CA als nationale Wurzelinstanz
- Teilnehmer:
  - Gateway-Administratoren
  - Marktteilnehmer (EMT)
  - Gateways

robotron®

BSI TR-03116 Teil 4

für u.a. § 52 Abs. 1

- Mindestvorgaben für verschiedene Aspekte der elektronischen Kommunikation
- TLS für Kommunikation über FTP und HTTP
  - Cipher-Suites
  - Signaturalgorithmen
- S/MIME für E-Mail-Kommunikation
- SAML für den Austausch von Authentisierungsinformationen z.B. Single Sign On
- Identifizierung
  - PKI-basiert
  - bilateraler Schlüsselaustausch und Web of Trust
- Regeln für kryptografische Schlüssel
- geringeres Sicherheitsniveau als Teil 3 (z.B. Hashfunktionen für Signatur)

robotron®

Agenda

1	▸ E-Mail und die Sicherheitsanforderungen
2	Alternative Technologien
3	▸ BDEW-Position
4	▸ Nächste Schritte

robotron®

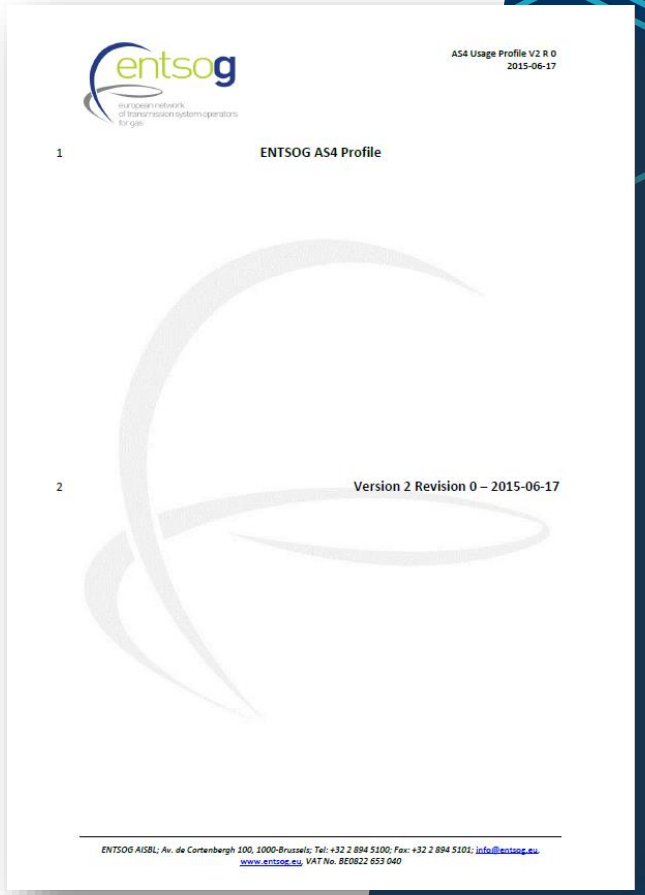
Technologien herkömmlich

- E-Mail
  - aktuell für MaKo im Einsatz - Normalfall
  - verschlüsselt und signiert - entspricht der BSI TR-03116 Teil 4
  - altbewährt
  - Zustellquittung (CONTRL) ansynchron – bis zu 6h
- AS2
  - aktuell für MaKo im Einsatz - Ausnahmefall
  - Verschlüsselt und signiert - entspricht der BSI TR-03116 Teil 4
  - konnte sich nicht durchsetzen
  - Zustellquittung synchron

Technologien zukünftig

AS4

- AS4
  - SOAP-Webservice (TLS)
  - verschlüsselt und signiert
  - Sammlung von Anforderungen und Standards
  - Genauere Ausdefinition erforderlich (usage profile)
- Einsatz für Fernleitungsnetzbetreiber auf europäischer Ebene (ENTSOG)
  - ENTSOG AS4 Profile
- Geeignet für alle digitalen Payloads - auch EDIFACT
  - ABER: Verschlüsselung und Signierung erfolgt mit XML-Encryption und XML-Signature
- Nichtabstreitbarkeit des Versands und des Empfangs

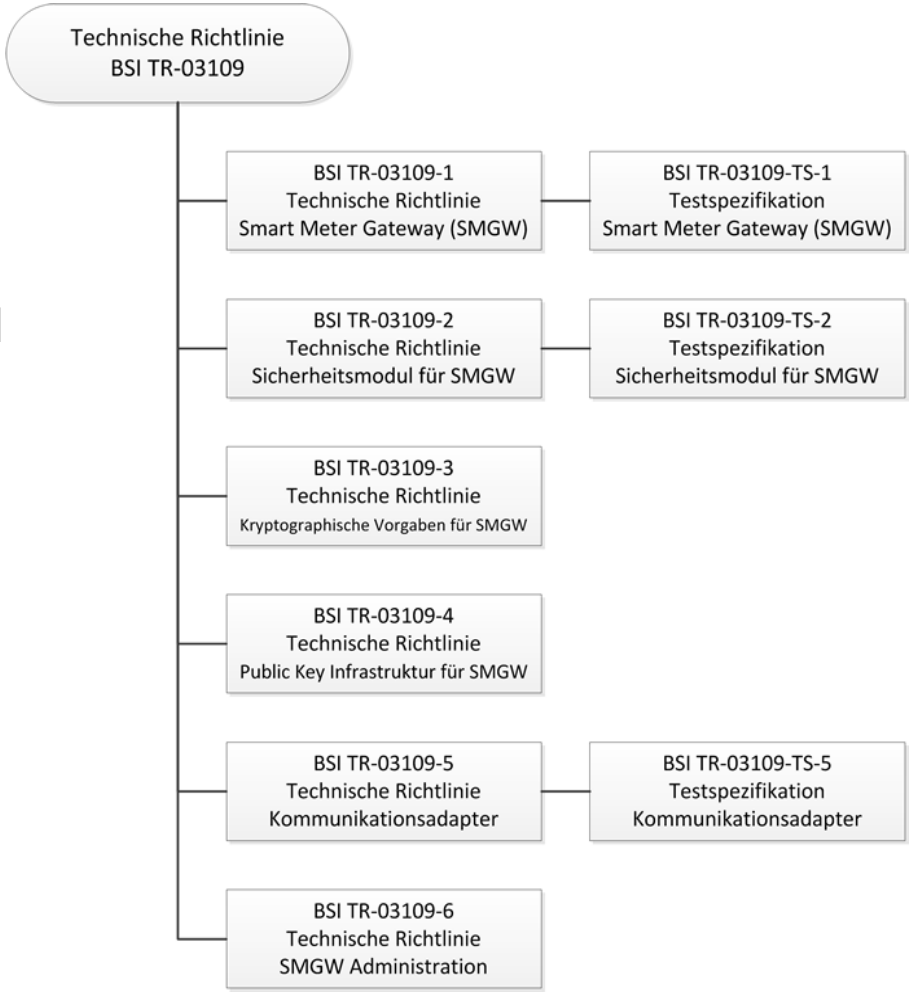


robotron®

Technologien zukünftig

SM-PKI

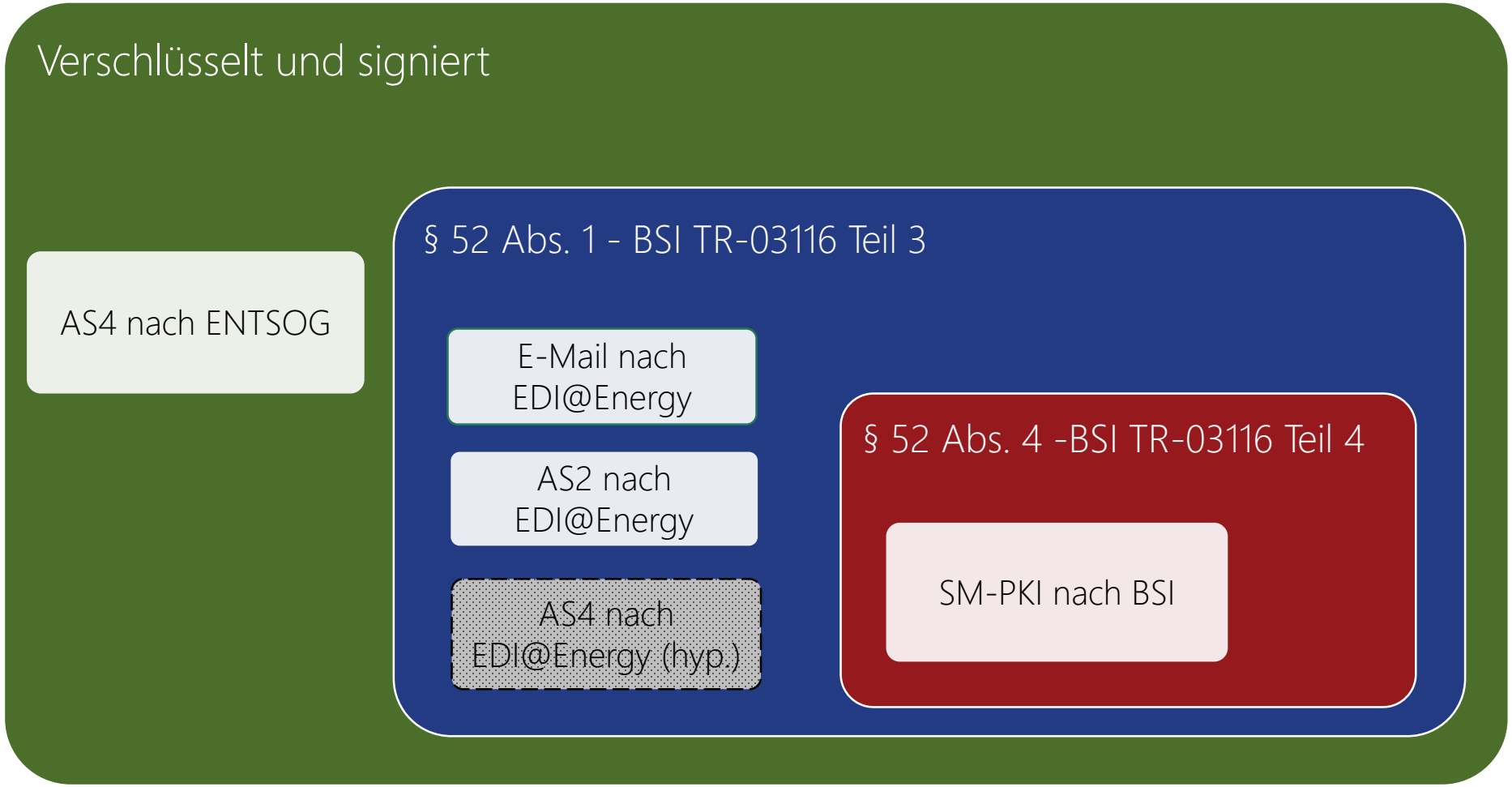
- beschrieben in BSI TR-03109
- RESTful-Webservice (TLS)
- CMS- Inhaltsdatensicherung
  - verschlüsselt und signiert laut BSI TR-0311 Teil 3
- Zertifikate von den Sub-CAs einer zentralen Root-CA
- Hardwaresicherheitsmodul (HSM)
- Geeignet für alle digitalen Payloads – auch EDIFACT
- Nichtabstreitbarkeit des Versands und des Empfangs



Quelle: BSI TR-03109-4_PKI, Version 1.2.1, BSI, 09.08.2017

robotron®

Technologien und Richtlinien



robotron®

Agenda

1	E-Mail und die Sicherheitsanforderungen
2	Alternative Technologien
3	**BDEW-Position**
4	Nächste Schritte

robotron®

Positionspapier

- vom 01.10.2018
- Positionsbestimmung zur Neuregelung der Marktpartner-Marktkommunikation

	SM- PKI (u.a. Zertifikate)	*Kryptographische Basisanforderungen*	*Übertragungsweg*	*Datenformat für Signatur- und Inhaltsverschlüsselung*
Szenario 1	*Ja*	*TR 3116-3*	*SMGW Webservice*	*CMS*
Szenario 2	*Nein*	*TR 3116-4*	*AS4*	*XML-SIG / XML-Enc*

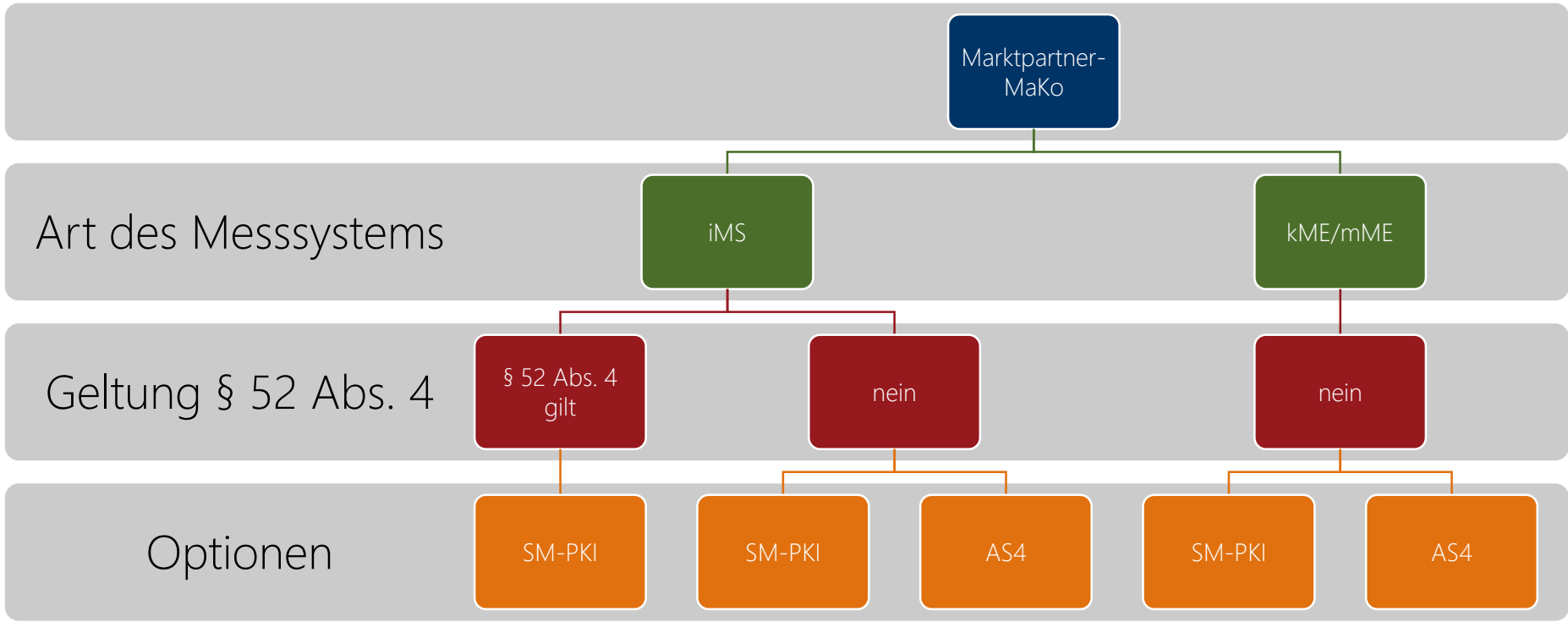
Quelle: Positionspapier Technologien in der Marktkommunikation, BDEW, 01.10.2018

- BDEW präferiert Szenario 2 mit Zertifikaten aus Sub-CAs einer Root-CA

robotron®

BDEW-Position im Lichte des MsbG

- § 52 Abs. 4 MsbG
  - Aus intelligenten Messsystemen stammende personenbezogene Daten, Stammdaten und Netzzustandsdaten dürfen nur zwischen Teilnehmern an der Smart-Metering-Public-Key-Infrastruktur des Bundesamtes für Sicherheit in der Informationstechnik kommuniziert werden […]



robotron®

Vergleich der Szenarien

	Szenario 1 – SM-PKI	Szenario 2 – AS4
Technologie ohnehin erforderlich für	MSB ÜNB LF NB	FNB
bewährte Technologie	nein	ja
angepasste Beschreibung und Implementierung notwendig	ja	ja
Basisanforderungen	BSI TR 3116-3	BSI TR 3116-4
eine Root-CA	ja	ja

Agenda

1	▸ E-Mail und die Sicherheitsanforderungen
2	▸ Alternative Technologien
3	▸ BDEW-Position
4	Nächste Schritte

Dez.2018 Abstimmung zwischen BDEW, BSI und BNetzA

Szenario 3?

robotron®

Die E-Mail ist tot, es lebe der Webservice?

Die Entscheidung steht noch aus.

Sicherheitsanforderungen

BSI TR 3116-3 oder BSI TR 3116-4

zwei Vorschläge des BDEW

AS4 oder SM-PKI

Das Ende der E-Mail ist nicht das Ende von EDIFACT.

robotron®

Ralf Teutsch / Leiter Entwicklung WPM
ralf.teutsch@robotron.de

www.robotron.de

MIT DATEN MEHR BEWEGEN.

robotron®

MIT DATEN MEHR BEWEGEN.

robotron®