deutsches forschungsnetz

Aktuelles zu Security, Trust & Identity Services

DFN-Betriebstagung | 06.10.2026

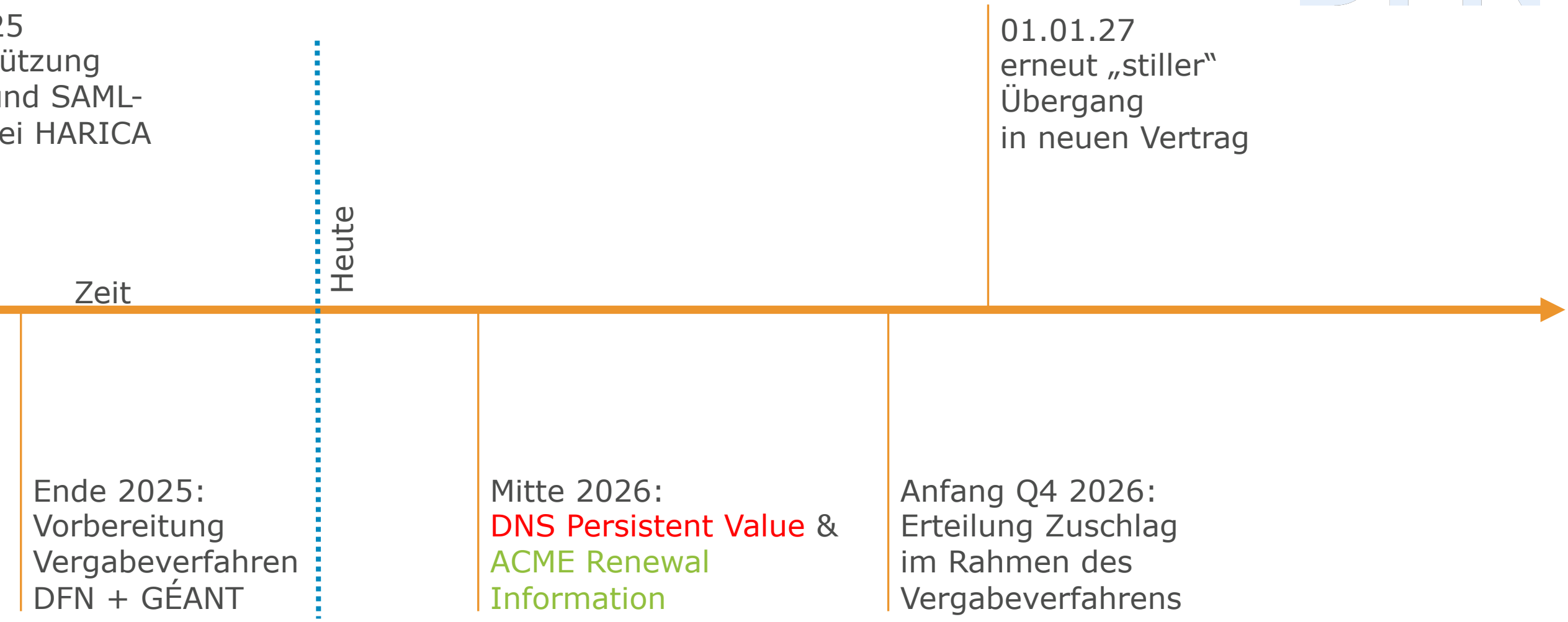
Ralf Gröper

DFN-PKI

Übergang Sectigo → HARICA



Übergang HARICA → ?



…und wer ist „?“

- Vergabeverfahren ist noch nicht 100% abgeschlossen, daher darf der neue Anbieter noch nicht genannt werden

…und wer ist „?“

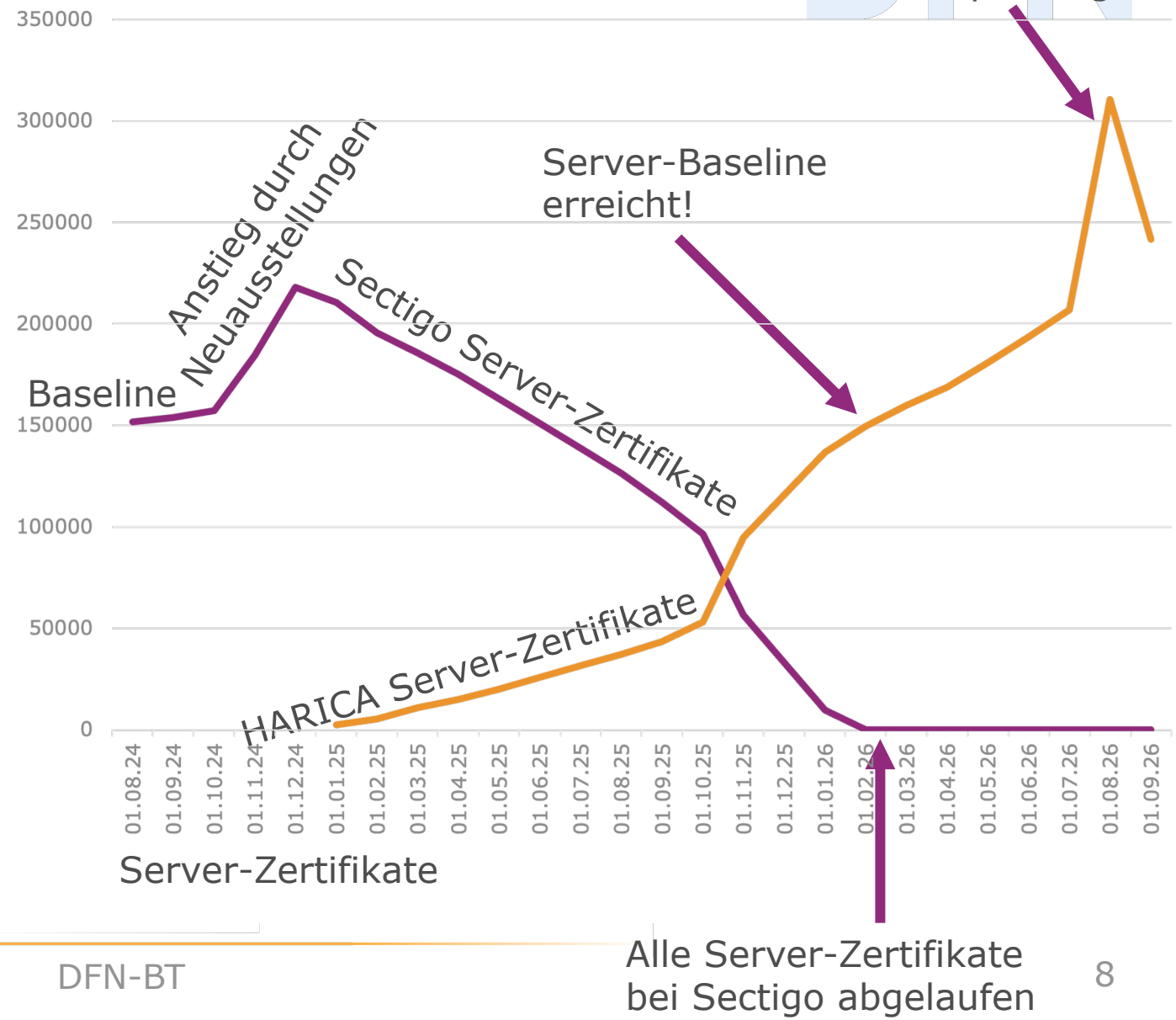
- Vergabeverfahren ist noch nicht 100% abgeschlossen, daher darf der neue Anbieter noch nicht genannt werden

- Daher nur so viel dazu…



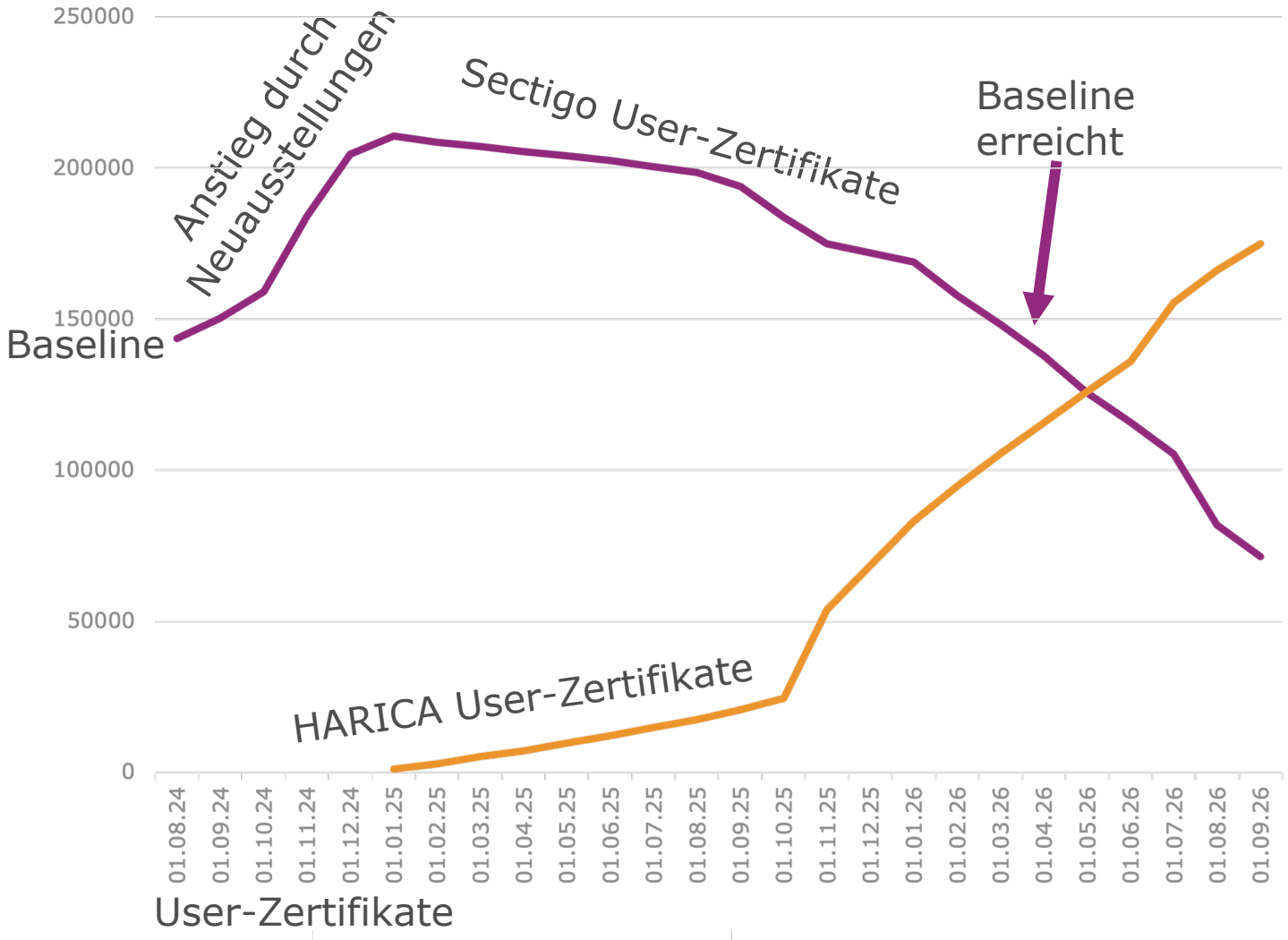
Übergang Sectigo → HARICA: Aktueller Stand

- **Gesundes Wachstum** bei HARICA von Anfang an
- Viele Einrichtungen haben Ende letzten Jahres auf unseren Rat hin alle Zertifikate bei Sectigo noch mal **neu ausgestellt**, Baseline daher Anfang Oktober 2024
- Wir erwarten ein **Einpendeln der Zahlen** in ähnlichen Bereichen wie bei Sectigo
  - Server-Zertifikate seit **Anfang 2026 abgeschlossen**
  - User-Zertifikate bis **Anfang 2028**



Übergang Sectigo → HARICA: Aktueller Stand

- **Gesundes Wachstum** bei HARICA von Anfang an
- Viele Einrichtungen haben Ende letzten Jahres auf unseren Rat hin alle Zertifikate bei Sectigo noch mal **neu ausgestellt**, Baseline daher Anfang Oktober 2024
- Wir erwarten ein **Einpendeln der Zahlen** in ähnlichen Bereichen wie bei Sectigo
  - Server-Zertifikate seit **Anfang 2026 abgeschlossen**
  - User-Zertifikate bis **Anfang 2028**



Massensperrungen bei HARICA

- **~90.000 Serverzertifikate** von DFN-Teilnehmern mussten im Juli von HARICA innerhalb von 5 Tagen **gesperrt** werden

- Warum? Von meinen Folien der letzten BT:

  - Hü und Hott: Entfall von **ClientAuth**-Key Usage in Serverzertifikaten
    - erst Sommer 2026, jetzt März 2027

- Deswegen… Mehreren CAs sind in dem „Hü und Hott“ ihre **Policies und Zertifikatprofile** auseinandergelaufen, auch HARICA

Massensperrungen bei HARICA

- Details zu den **konkreten Hintergründen** im Forum Sicherheit von Reimer Karlsen-Masur

- Hier nur so viel:

Vielen Dank für Ihre Geduld und konstruktive Mitarbeit!

- **Verständlich Frage**: Ist ein Anbieter, der solche Massensperr-Events verursacht, eigentlich der richtige – oder gibt es bessere?
  - Schauen wir doch mal → https://webpki.systematicreasoning.com/#ops

…und sonst so?

- **Zeitstempeldienst**: Wir hatten letztes Mal angekündigt, den Zugriff auf DFN-Teilnehmer zu beschränken.
  - Das haben wir erst einmal vertagt und überlegen noch einmal grundsätzlich, ob und wie das sinnvoll möglich ist.

- **Automatisierung**:
  - Laufzeiten für Serverzertifikate werden weiter verkürzt
  - Seit März 2026: 199 Tage
  - Ab März 2027: 100 Tage
  - Bitte automatisieren Sie!

- **Hilfreiche Werkzeuge** zur Automatisierung:
  - **ACME** + **ARI** + ggf. **Validierung per DNS persistent Value**
    - Domainvalidierung per DNS Persistent Value leider noch nicht produktiv (Gründe: Tonspur…)

DFN-Security

Ausblick: Der Netzwerkprüfer 2.0

- Der Netzwerkprüfer ist eines der **ältesten Leistungsmerkmale** des DFN-Security Dienstes

- Ziele:
  - **Außensicht auf das eigene Netz**, primär offen erreichbare Serverports (vgl. nmap)
  - Für sehr kleine Netzbereiche auch **eingeschränkter Schwachstellenscan** möglich (vgl. OpenVAS)

- Ergebnisse per **Mail** und im **Security-Portal** abrufbar
  - regelmäßige Scans als „Diff" zu vorhergehenden Scans dargestellt
    - Auf einen Blick sehen, ob neue Ports dazu gekommen sind
    - Insbesondere für Soll-Ist-Vergleich im Rahmen des ISMS geeignet

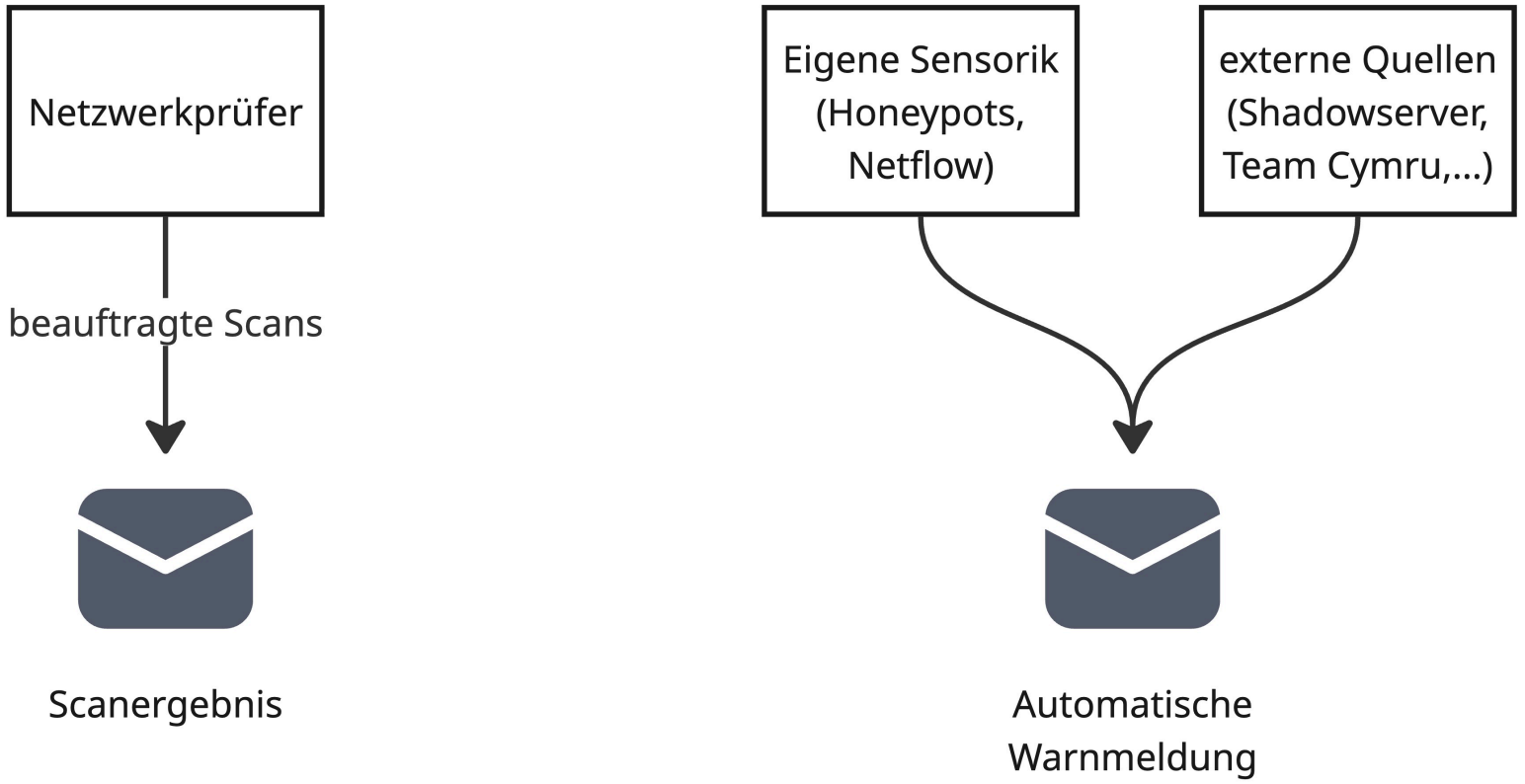
Der Netzwerkprüfer

- Das **Backend des Netzwerkprüfers** ist im Spätherbst seines Lebenszyklus
  - Hat jahrelang (Jahrzehnte…) gute Dienste geleistet
  - Inzwischen mit Abhängigkeiten, die nicht mehr zeitgemäß sind

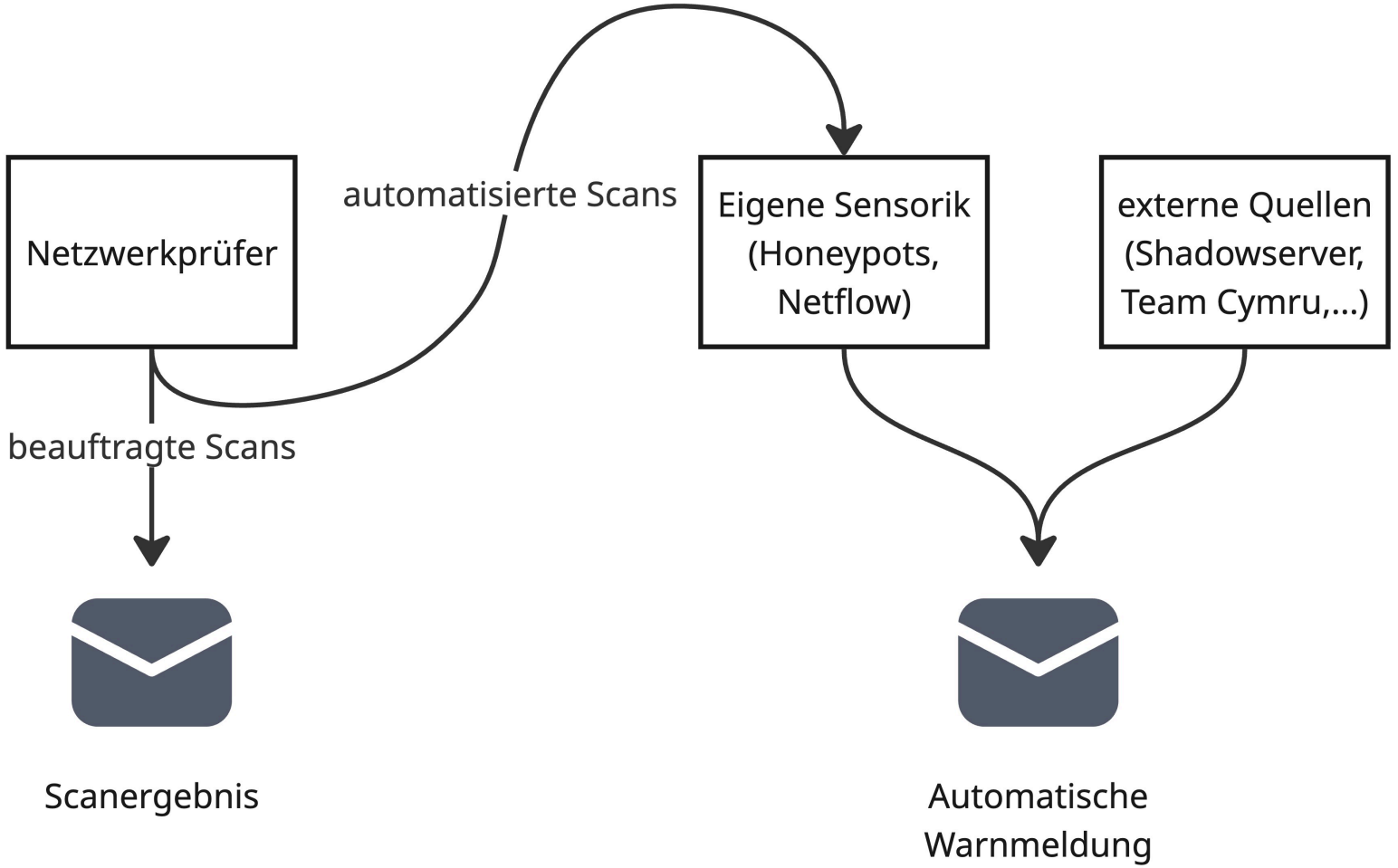
- Netzwerkprüfer wird also **geplant** und turnusmäßig **abgelöst**
  - Das nehmen wir zum Anlass, auch das **Featureset** neu zu bewerten und den Netzwerkprüfer neu auszurichten
  - Insbesondere: Einsatz als **automatisierte Sensorik** zusätzlich zu manuell beauftragten Scans

- Idee: In **3 Stufen** neu aufbauen und dabei **erweitern**
  - Leichtgewichtige Scans vollautomatisieren und in die Breite bringen
  - Erweiterte Möglichkeiten für Tiefenscans

Aktuell: Keine Verbindung zwischen Netzwerkprüfer und Automatischen Warnmeldungen



Zukünftig: Netzwerkprüfer agiert zusätzlich als Sensorik für Automatische Warnmeldungen



1. Stufe Ausbau Netzwerkprüfer

- Aufbau **neuer Scanknoten** neben den bestehenden (alten) Scanknoten

- Neue Scanknoten **scannen** im X-WiN **proaktiv**
  - Fokus auf **nichtinvasive Scans**
  - Auslieferung von erkannten potentiellen Sicherheitsproblemen über **Automatische Warnmeldungen** an **alle** Teilnehmer
    - Unabhängig von eigenen konfigurierten Scans

- Über das DFN-Security Portal **manuell beauftragte Scans** laufen zunächst weiterhin auf der alten Plattform

- Beginn **dieses Jahr**

2. Stufe Ausbau Netzwerkprüfer

- Migration der über das DFN-Security Portal **beauftragten Scans** auf die **neue Scanplattform**, Abschaltung der alten Plattform
- Moderat **erweiterte Features** bspw. bei den Scans auf Schwachstellen
- Beginn **nach Phase 1** – voraussichtlich 2027
  - Softwareentwicklung im DFN-Security Portal notwendig

3. Stufe Ausbau Netzwerkprüfer

- Erweiterung und **Einbindung des** (bestehenden) **SOC-Connectors** als **On-Premise-Scanknoten** für über das DFN-Security Portal konfigurierte **Tiefenscans**
  - Aktuell dient der SOC-Connector ausschließlich der Logdatenanalyse, war aber von Anfang an auf Erweiterbarkeit ausgelegt
- On-Premise Tiefenscans erlauben deutlich **weitergehende Scanoperationen**
  - Alternative oder **Ergänzung zu eigener Sensorik** (OpenVAS, Greenbone,…)
- Beginn **nach Phase 2** – Zeitpunkt aktuell offen

…und sonst so?

- **MISP** – Plattform für Communities zum Austausch von **Malware Information** (IoCs, Threat Intelligence)
  - Jetzt auch beim DFN, in zwei Geschmacksrichtungen:
    1. Selbstbetrieben, förderierter Informationsaustausch mit DFN-Instanz
    2. Mandant auf DFN-CERT MISP – niedrigere Einstiegshürde
  - MISP **Informationsveranstaltung** - Nächster Termin: 04.11.2026 10:30 -11:30

- **DFN-Dienste** zur Ausgestaltung der **Bausteine** / **Controls** von ISMSen
  - Mapping auf **BSI IT-Grundschutz** verfügbar
    - https://www.dfn.de/bsi-it-grundschutz-bausteine/
  - Mapping auf **ISO 27.001-Controls** fast fertig (Dank an die AKIF-Community!)

DFN-Dienste als IT-Grundschutz-Bausteine

Stand: Mai 2026

DFN-Dienste	IT-Grundschutz-Baustein	Anforderung(en)	Wirkung
DFN-Security (Basis- und erweiterte Leistungen)			
Security Incident Management durch das Incident Response Team (IRT)	DER.2.1 (Behandlung von Sicherheitsvorfällen)	A3, A4, A5, A6, A7, A8, A9, A10, A14, ggf. A20/21	unterstützend
	DER.1 (Detektion von sicherheitsrelevanten Ereignissen)	A3	unterstützend
Logdaten-Analyse	OPS.1.1.5 (Protokollierung)	A6, A9	als Bestandteil der zentralen Protokollierungsinfrastruktur
	DER.1 (Detektion von sicherheitsrelevanten Ereignissen)	A6, A11, A12, A14, A15	unterstützend, ggf. umgesetzt
Schwachstellenmeldungen	OPS.1.1.3 (Patch- und Änderungsmanagement)	A1	unterstützend
	DER.1 (Detektion von sicherheitsrelevanten Ereignissen)	A12	unterstützend, ggf. umgesetzt

Mehr zu den Themen Security & PKI

Forum Sicherheit: heute, 13:30 bis 15:30

Forensprecher: Stefan Kelm (DFN-CERT)

1. Neues aus dem DFN-CERT
   - T. Kahl (DFN-CERT)
2. Neues aus der DFN-PKI
   - R. Karlsen-Masur (DFN-CERT)
3. Perspektive Web-PKI
   - J. Brauckmann (DFN-CERT)
4. Warum sind LLM (un)sicher?
   - J. Kohlrausch (DFN-CERT)

Neues aus der DFN-AAI

- **Schulungen**
  - Workshop Shibboleth IdP für Fortgeschrittene am 17. und 19. November
  - Halbtägige Info-Veranstaltung zur DFN-AAI für Anfang Dezember geplant
- **DFN edu-ID**
  - Diverse kleinere Baustellen, vor allem unter der Haube
  - Pilotbetrieb voraussichtlich noch bis Anfang 2027
- **NFDI-Basisdienst IAM** (IAM4NFDI)
  - Anbindung an EOSC AAI Federation
- DFN ist Projektpartner in **EOSC4ALL** – Start am 1.9.2026
- Details hierzu im Forum AAI mit Wolfgang Pempe

Mehr zur zum Thema AAI

Forum AAI heute 16:00 bis 18:00

Forensprecher: Steffen Hofmann, FU Berlin

1. Neues aus der DFN-AAI
   - W. Pempe (DFN-Verein)
2. ~~How to deal with entitled users at my university – Autorisierung mittels Entitlement-Strings~~
   - ~~A. Lackner (Universität Bonn)~~
3. Shibboleth IdP mit eduMFA containerisiert betreiben
   - D. Hübner (DAASI International GmbH)
4. KI-gestützte Freigabe von Serviceprovidern – ein Experiment
   - J. Nehlsen (Digitalverbund Bayern im Hochschulbereich)



Mehr zum Thema eduroam & co.

Forum Mobile IT: morgen, 11:30 bis 13:30

Forensprecher: Markus Krieger (Uni Würzburg)

1. Neues zu eduroam
   - J.-F. Rieckers (DFN-Verein)
2. ~~Neues zu easyroam~~
   - ~~R. Paffrath (DFN-Verein)~~
3. Toying around with OpenWifi in edu environments
   - S. Klemer (GWDG)

Übersicht

Uhrzeit	Forum
Heute, 13:30 – 15:00 Uhr	Forum Sicherheit (DFN-PKI & DFN-Security)
Heute, 16:00 – 18:00 Uhr	Forum AAI (DFN-AAI)
Morgen, 11:30 – 13:30 Uhr	Forum Mobile IT (eduroam & co.)