80. DFN Betriebstagung - VoIP

DFN VoIP Centrex mit NFON
von der Planung bis zur Umsetzung

Agenda

- Was war?
- Was ist?
- Was wird?

Who is who

- **GFZ -** Helmholtz-Zentrum Potsdam - Deutsches GeoForschungsZentrum GFZ
- **NuGem – Nu**tzer**gem**einschaft des Telegrafenbergs bestehend aus GFZ, PIK, AWI, AIP & DWD
- **NFON -** NFON AG
- **Telekom –** Deutsche Telekom Business Solutions GmbH

- ca. 4500 Räume
- ca. 130 Gebäude
- ca. 2000 Nebenstellen
- 4 Standorte

Was war?

- Alcatel-Lucent Omni PX Enterprise – Telefonanlage
  - Wartung und Konfiguration über lokalen externen Dienstleister
  - 2018 auf neuesten Stand bringen um Zeit zu verschaffen für VoIP Einführung
  - 2018: ~80 TEUR – danach jährlich ~30 TEUR
- 2 Multiplexer mit jeweils 30 Kanälen → 60 gleichzeitige ein/ausgehende Anrufe
  - Innerhalb von 20 Jahren nur einmal das Limit erreicht
  - **ABER:** künftig sollte diese Beschränkung wegfallen (niemand konnte Corona und den plötzlichen Hype von Zoom usw. vorhersehen)
- 100 OpenTouch Multimedia Services Lizenzen
  - händisch verwaltet, keine Anbindung an vorhandene IT-Infrastruktur (Authentifizierung, LDAP, …)
  - Windows only

Was war?

- **Kopfnummer** 03 31 / 288 - 0 bis 2999
- Wildwuchs in der NuGem
  - kein Block für GFZ VoIP Lösung

➢ Neue Kopfnummer für GFZ

  ➢ 0331 / 6264 – 0 bis 3999

Ihr Zeichen, Ihre Nachricht vom	Mein Zeichen, meine Nachricht vom	Telefon	Mainz,
20.01.2021	114-2 / 4/2021	06131 18-1142	25.01.2021

Bescheinigung des Rufnummernbedarfs nach Methode 2 der Amtsblattverfügung 25/2006

Sehr geehrte Damen und Herren,

unter der Voraussetzung der von Ihnen im o.g. Antrag genannten Bedarfsangaben bestätige ich Ihnen hiermit den Bedarf von insgesamt

4000 Endeinrichtungsnummern.

Diese Bescheinigung gilt ausschließlich für den u.g. Standort und den nachstehend aufgeführten Bedarfsangaben:

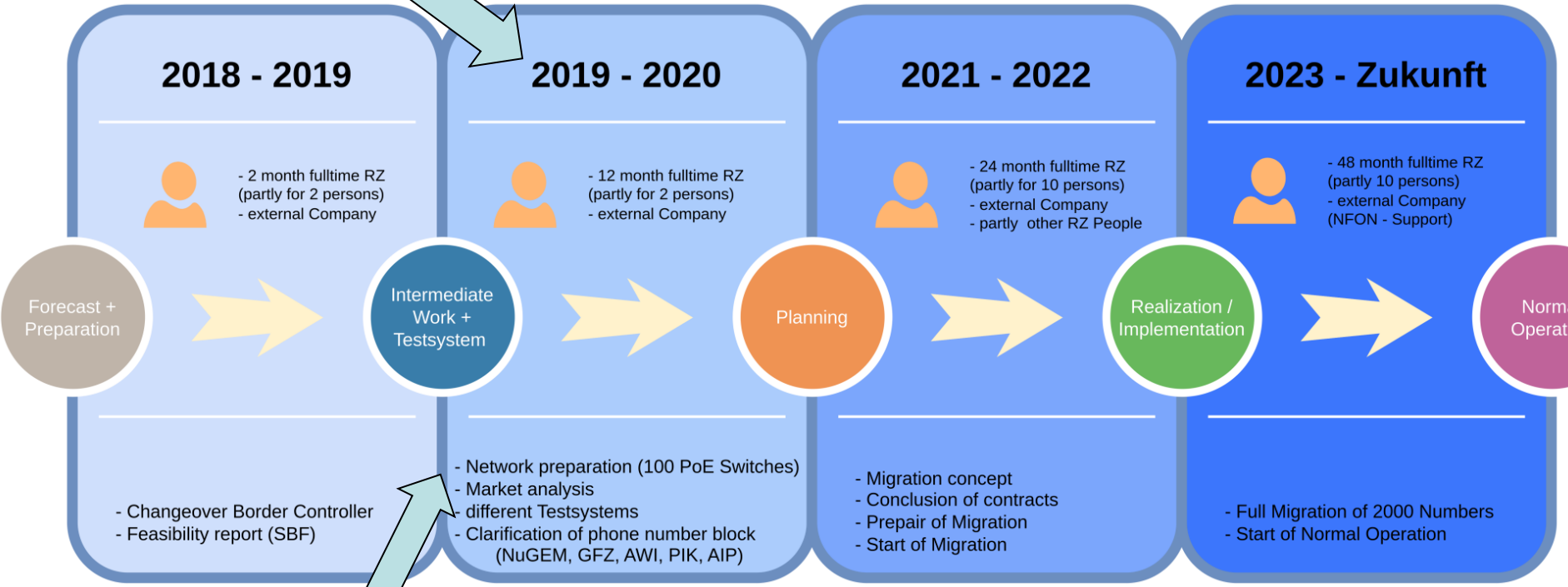
Telegrafenberg
14473 Potsdam

Basisanschlüsse	0
Primärmultiplexanschlüsse:	0
Parallele SIP-Sessions:	64
Derzeit vorhandene Nebenstellen:	2000
Geplante Erweiterung auf insgesamt:	4000

Sie dient zur Vorlage an Ihren Netzbetreiber.

NFON Teststellung

Was ist (gewesen)?

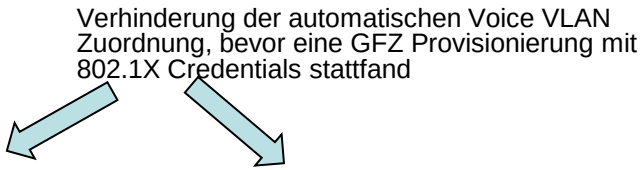


externes Gutachten mit Kostenanalyse durch D.I.E. PROJEKT GmbH (Dresden) für den Vorstand

Quelle: Andreas Schoe (GFZ)

Was ist (gewesen)?

Was ist?



- CISCO Catalyst 3650 Switches (LLDP *transmit* & CDP **deaktiviert**)
- IEEE 802.1X via Kupfer optional (VLAN über Radius Server)
- VLAN Matrix entsprechend der Organisationsstruktur
  - Maximal 8 Departments mit jeweils 8 Sektionen (aktuell 6 + 2 mit jeweils 4-6 Sektionen) = 64 Sektions VLANs + 1 VoIP VLAN + ….
  - Sektionen größtenteils in Gebäuden / Etagen zusammengefasst
  - Switch-Port Konfiguration individuell mit untagged VLAN (Access Port)
- Yealink T51, T53W, T54W
  - Pre-Provisionierung möglich via lokalem TFTP / HTTP
  - 802.1X via PEAP-MD5 → keine MAC-Listen am RADIUS

Was ist (mit Provisionierung)?

- 5 Bootvorgänge bis Telefon abschließend einsatzbereit
- Keine Staging-Area notwendig
- Zustellung der Telefone an zentrale Warenannahme
- Ausliefern der Telefone durch Hausmeister
- Anschluss der Telefone durch Mitarbeitende (*theoretisch*)
- Hilfevideos & Umfrage zur Auswahl Tischtelefon/Softphone
  - 70% Tischtelefone

Was ist (mit Provisionierung)?

- 1. Bootvorgang
  - kein 802.1X → VLAN ID = PVID (Access Port VLAN) → eingeschränkter Zugriff
    - mind. NTP / Yealink Server / GitLab (intern) notwendig
  - DHCP Anfragen vom Telefon nach Option 66 (TFTP / HTTP Server) & 132 (802.1Q VLAN ID) werden ignoriert
  - ➢ Firmware Update durch Yealink Server
- 2. Bootvorgang
  - kein 802.1X → VLAN ID = PVID (Access Port VLAN) → eingeschränkter Zugriff
  - DHCP Anfragen durch Yealink Telefon nach
    - Option 66 (TFTP / HTTP Server) → interner Provisionierungsserver (**GitLab Pages**)
    - Option 132 (802.1Q VLAN ID) → ignoriert vom DHCP Server
  - Zukünftige HTTP Anfragen an <URL> (**GitLab Pages**)
    1. <URL>/{MAC}.boot → 404
    2. <URL>/y000000000000.boot → include:config „encryption.cfg" & overwrite_mode = 1
    3. <URL>/encryption.cfg

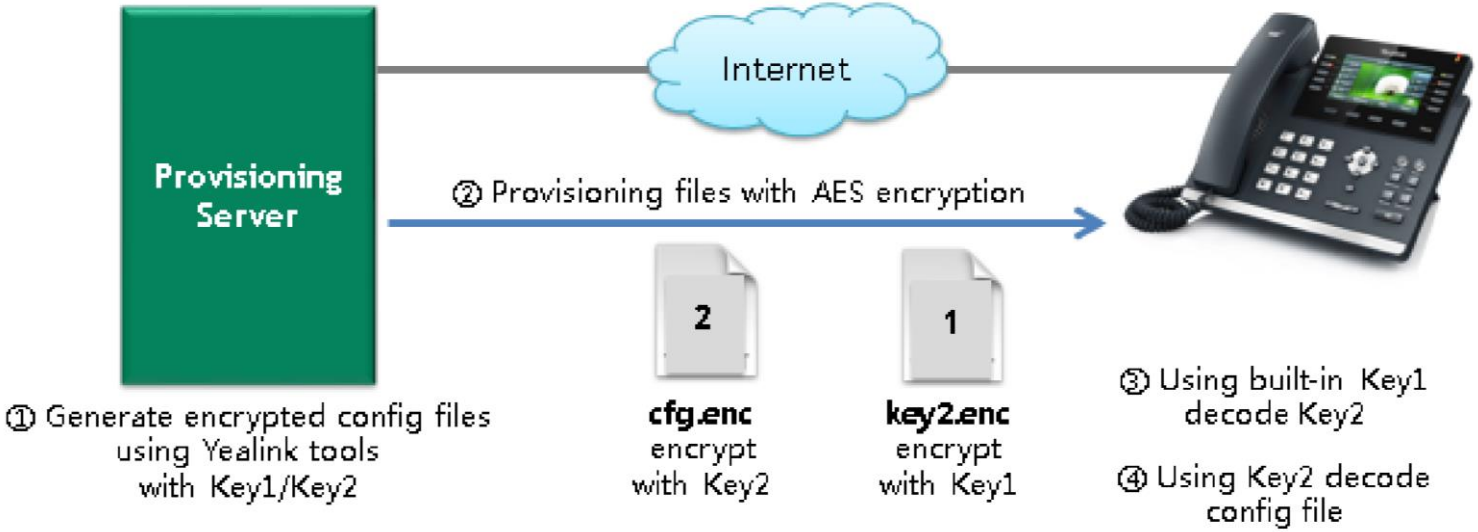
encryption.cfg

```
#!version:1.0.0.1
## The header above must appear as-is in the first line

# Enable the IP phone to decrypt configuration files using the encrypted AES keys
static.auto_provision.aes_key_in_file = 1

# Use this static provisioning url pointing to the encrypted configuration files
static.auto_provision.server.url = http://voip.git-int-pages.gfz-potsdam.de/yealink-provisioning/encrypted/

# Ignore the provisioning URL given by DHCP Option 66 (TFTP Boot)
static.auto_provision.dhcp_option.enable = 0

# Force reboot after applying these settings, to load encrypted files and AES keys
static.auto_provision.reboot_force.enable = 1
```

Was ist (mit Provisionierung)?

- 3. Bootvorgang
  - kein 802.1X → VLAN ID = PVID (Access Port VLAN) → eingeschränkter Zugriff
  - DHCP Anfragen durch Yealink Telefon nach
    - Option 132 (802.1Q VLAN ID) → ignoriert vom DHCP Server
  - Download der GFZ Konfigurationen von vorher übermittelter <URL>
    1. GET http://voip.git-int-pages.gfz-potsdam.de/yealink-provisioning/encrypted/{MAC}.boot → HTTP 404
    2. GET http://voip.git-int-pages.gfz-potsdam.de/yealink-provisioning/encrypted/y000000000000.boot → include:config "encryption.cfg"
    3. GET http://voip.git-int-pages.gfz-potsdam.de/yealink-provisioning/encrypted/gfz.cfg → via yealinkencrypt verschlüsselt – enthält 802.1X PEAP MD5 Credentials
    4. GET http://voip.git-int-pages.gfz-potsdam.de/yealink-provisioning/encrypted/gfz_Security.enc → via yealinkencrypt erzeugter, built-in Public Key verschlüsselter Schlüssel zum entschlüsseln der gfz.cfg

Was ist (mit Provisionierung)?



y000000000000.boot

```
#!version:1.0.0.1
## The header above must appear as-is in the first line

include:config "gfz.cfg"

include:config "http://rds.cloud-cfg.com/yealink/y000000000000.boot"
include:config "http://rds.cloud-cfg.com/yealink/$mac.boot"

…
[T54W]include:config "http://rds.cloud-cfg.com/yealink/y000000000096.cfg"
[T53W, T53]include:config "http://rds.cloud-cfg.com/yealink/y000000000095.cfg"
…
include:config "http://rds.cloud-cfg.com/yealink/$mac.cfg"

overwrite_mode = 1
specific_model.excluded_mode = 0
```

gfz.cfg

```
#!version:1.0.0.1
## The header above must appear as-is in the first line

# 802.1x MD5 credentials
static.network.802_1x.mode = 1
static.network.802_1x.identity = VOIP
static.network.802_1x.md5_password = 🔑🔑🔑🔑🔑🔑🔑🔑🔑🔑🔑

# Getting Voice VLAN via non-default DHCP Option 224
# reserved for private use according to IANA
static.network.vlan.dhcp_enable = 1
static.network.vlan.dhcp_option = 224
```

Was ist (mit Provisionierung)?

- 4. Bootvorgang
  - 802.1X → Voice VLAN ID = 632 (via RADIUS Authentication)
  - DHCP Anfragen durch Yealink Telefon nach
    - Option 66 (TFTP / HTTP Server) → → ignoriert vom DHCP Server
    - Option 224 (GFZ Custom) → Voice VLAN ID via DHCP → Telefon taggt selbstständig
      - DHCP Server kann somit unterscheiden, ob Telefon bereits authentifiziert & provisioniert ist
  - Download der NFON Konfigurationen von NFON Servern
- 5. Bootvorgang
  - Provisionierung abgeschlossen
  - Telefon bereit zur Anmeldung einer Nebenstelle

- Nach Werksreset beginnt der Prozess beim 2. Bootvorgang

Was ist (mit den Nutzenden)?

- Informationsveranstaltung zur Umstellung auf IP-Telefonie
  - Zoom Webinar am 13.12.2022 („dank" Corona – Nutzende deutlich offener für ein solches Format)
  - Inhalte:
    - Kurze Erklärung, was IP-Telefonie ist
    - Ablauf der Umstellung am GFZ
    - Gemeinsamkeiten mit aber auch Unterschiede zu der bisherigen Telefonie
    - Kurze Vorführung der neuen Telefone und weiteren Möglichkeiten zum Telefonieren
- Video zur Entscheidungshilfe Tischtelefon vs. Softphone
  - Inhalte:
    - Kurze Erklärung Softphone
    - Unterschiede zwischen der Nutzung der Tischtelefone und der Softphones
    - Unterschiede zu den alten Telefonen
    - Besonderheiten während der Zeit der Umstellung am GFZ
- Umfrage bei der sektionsweisen Umstellung nach Bedarf
  - Bestellung von Telefonen bei NFON via Hochrechnung nach 5 Sektionen
- Showroom mit den 3 Telefonen (T53W,T54W,T57W) → mäßige Nachfrage

Was ist (mit NFON)?

- Exzessive Nutzung der REST-API (auch ohne SLA)
  - Schwieriger Einstieg
  - Dokumentation nicht intuitiv
  - ABER: Wenn es läuft, läufts (im Gegensatz zu Sectigo und Serverzertifikaten)
- Mehrstufige BASH-Scripte (Beispiel Nutzerprovisionierung)
  1. CREATE phone-extensions (Nebenstelle erzuegen)
  2. CREATE inbound-trunk-numbers (eingehende Rufnummer erzeugen)
  3. PUT phone-extensions (blacklistProfile)
  4. PUT voice-mail (PIN Generierung @ GFZ → Zustellung per E-Mail)
- Provisionierung von Softphone Zugängen leider nur manuell über WebUI → Nutzende erhalten Zugangslink von NFON

Was wird?

- Network Access Control (NAC) forcieren
  - Funktioniert unser bisheriges genauso weiter, wie es geplant war?
  - Wird DHCP Option 224 evtl. obsolet, da VoiceVLAN Zugriff auf Provisionierungsserver erhält?
- Softphone Zugänge automatisiert provisionieren
  - NFON arbeitet dran
  - sind gerne Early Adaptor!
- Umstellung von ~130 analogen Restgeräten
  - davon ~30 Faxgeräte (schon vor Jahren per Vorstandsbeschluss verboten)
  - Modems, DECT, Türsprechanlagen
- Umstellung vorhandener SIP Türsprechanlagen
  - „unprovisioned SIP Device“
  - Kein SLA
  - NDA unterzeichnen bei NFON