designing e-health

Netzwerkdokument GINS

für

ecard Services

Eine technische Beschreibung für VP-/IT-Dienstleister

Version: 5.0.18

Status: freigegeben

Datum: 06.05.2024

Inhaltsverzeichnis

1 Dokumenten-Informationen 4

1.1 Ziel und Inhalt des Dokuments 4
1.2 Dokument Historie und Status 5
1.3 Kontaktinformation 5

2 Grundlagen GIN (Gesundheits-Informations-Netz) 5

2.1 Schematischer Aufbau und Komponenten 6
2.2 Die Kommunikations-Schnittstellen der GIN-Services 8
2.3 Zuständigkeiten und Schnittstelle im VP-LAN 8
2.3.1 Kurzbeschreibung der Leistungen des GIN-Zugangsnetz-Providers 9
2.3.2 Übergabe des Zugangs durch den Provider 10
2.4 Grundlagen der Kommunikation im GIN 11
2.5 Frei erreichbare Portale im GIN 12
2.6 Sicherheitsaspekte (informell) 12
2.6.1 Sicherheit der Kommunikations-Wege 13
2.6.2 Sicherheit des Zugangsrouters und des GINO 13
2.6.3 Verschlüsselung der Daten 13
2.6.4 Prüfung der Anschluss- bzw. Request-IP-Adresse 14

3 IP-Adressvergabe und Schema für das Netzwerk des VPs 15

3.1 Adresszuordnung für den VP 15
3.2 SV-Adressbereich 16
3.3 MWD-Adressbereich 16
3.4 Netz für das LAN des VP (alias Ordinations-LAN) 17
3.5 Eigenes lokales IP Netz 18
3.6 Freigegebene IP-Netze für das LAN des VP 19
3.7 DHCP Einstellungen – LAN des VP 19
3.7.1 Übersicht zur DHCP Konfiguration im LAN des VP 20
3.7.2 DHCP Parameter 20
3.7.3 Alternative Konfigurationen zum Standard DHCP 22
3.7.4 DHCP im LAN des VP nicht gewünscht oder nicht möglich 22
3.7.5 Eigenes Netz – statisch oder mit DHCP 22
3.7.6 Ethernet-Interface und IP-Konfiguration GINO 23

4 GINO – Kommunikation und Konfiguration 24

5 Namensauflösung (DNS) im GIN und im VP-LAN 29

5.1 DNS-Server am PeeringPoint 29
5.2 DNS-Server beim VP 29
5.3 Internet DNS für die Auflösung von Services im GIN 29
5.4 Namensauflösung – GINA (obsolet) als DNS-Server – Folgen für die VP-Konfiguration 30
5.5 DNS-Forwarding durch den e-card-Router 30
5.6 Namensauflösung (DNS) für Mehrwertdienste 30
5.7 Namensauflösung mit lokalem DNS-Server im Netzwerk des VP 31
5.7.1 Schaubild Namensauflösung mit lokalem DNS 32
5.7.2 Verfügbarkeit und Zuständigkeit 33
5.8 Vorhandene DNS, DHCP – Dienste im Netzwerk des VP 34

6 Routing im Netzwerk des VP 36

6.1 Support und Zuständigkeit 36
6.2 Prinzip der Realisierung – Routing 37
6.3 Technische Randbedingungen und Anforderungen 39
6.4 Firewall (routing) (VP-LAN) 40
6.5 Routing mit lokalem Internetanschluss 41

6.6 E-CARD „REFERENZ-SYSTEM“ BEI ROUTING UND FIREWALLS 44
6.7 PRAXISBEISPIEL „NICHT FREIGEGEBENE IP-NETZE IM GDA-LAN“ – LÖSUNGSANSATZ MIT NAT AUF EINER FW ZWISCHEN DEN GDA-LANS. 45
6.7.1 1:1 NAT zwischen den beiden GDA-LANs 45
6.7.2 Hide-NAT (Overload-NAT) zwischen beiden VP-LANs 46
6.7.3 Routing auf der Firewall (für beide Varianten) 47
6.7.4 Generelle Anmerkungen zu diesem Praxisbeispiel 47
7 Firewall transparent (VP-LAN) 48
7.1 VP-LAN – KOMMUNIKATION MIT DEN SERVICES IM GIN (GINS) 49
7.2 VP-LAN – KOMMUNIKATION MIT MWD-SERVICES 50
8 Informationssammlung: „Fakten auf einem Blatt“ 51
8.1 ÜBERGREIFENDE SYSTEME 51
8.1.1 PP-DNS: 51
8.1.2 Routen/Netze ins/im GIN: 51
8.1.3 QoS 51
8.1.4 OCSP 52
8.2 VPSWH-UMGEBUNG 52
8.2.1 OCSP Service für Test-Referenzsysteme 52
8.2.2 ECARD/ELGA/TRANSFER-Services 52
8.2.3 MyIP-Auskunftsservice 52
8.2.4 NTP (gesichert) für GINOs 52
8.2.5 Freischaltungen VPSWH/Referenz-System 53
8.3 PRODUKTIONS-UMGEBUNG (VERTRAGSPARTNER) 55
8.3.1 OCSP Service 55
8.3.2 ECARD/ELGA/TRANSFER-Services 55
8.3.3 MyIP-Auskunftsservice 55
8.3.4 NTP (gesichert) für GINOs 55
8.3.5 Freischaltungen Produktiv-System 56
9 Abbildungsverzeichnis 58
9.1 ABKÜRZUNGEN 59

1 Dokumenten-Informationen

Dieser Abschnitt fasst die Grundinformationen des Dokuments zusammen, darunter: Version, Status, Inhalte etc.

1.1 Ziel und Inhalt des Dokuments

Das Dokument richtet sich an alle technischen Verantwortlichen, die für die Konfiguration des Netzwerkes und der Anwendungen im Netzwerk des VP (SV-Partner) zuständig sind, bzw. damit beauftragt werden.

Das Dokument ist auf den Zeitpunkt nach der Ablösung von GINA und LAN-CCR durch GINO und zentrale Services ausgelegt. Es wird allerdings auch auf die notwendigen Änderungen in Bezug auf GINA und LANCCR eingegangen.

Die erfolgreiche Nutzung der zentralisierten e-card-Services und des GINO an Stelle von GINA und LAN-CCR ist abhängig von der vorhandenen Infrastruktur (Netzwerk, Server, Dienste, Software) beim VP und bedarf eventuell einer Änderung durch den jeweils zuständigen bzw. durch den vom SV-Partner beauftragten Dienstleister.

Die Integration des e-card Service in die Netzinfrastruktur des VPs ist abhängig von der vorhandenen Infrastruktur (Server, Dienste, Software, Firewalls, Internetanschluss, Filialstandorte) und bedarf daher einer Vorbereitung durch den jeweils zuständigen bzw. durch den vom SV-Partner beauftragten Dienstleister.

Dieses Dokument kann nicht alle möglichen Varianten[1] darstellen.
Ziel ist es, die grundlegenden Randbedingungen darzustellen und die prinzipiellen Vorgehensweisen aufzuzeigen.
Diese exemplarischen Vorgehensweisen sollen dem Ausführenden der e-card-Integration in das Netz des VPs als Anleitung dienen und ein Beispiel für eine auf seine Situation passende Lösung sein.
Das Dokument fasst die notwendigen Parametrisierungen für das LAN und die Anbindung der lokalen Infrastruktur an das „Gesundheits-Informations-Netz“ (GIN) zusammen.

Dieses Dokument wird regelmäßig fortgeschrieben und aktualisiert.

[1] Das Dokument beschreibt nur häufig verwendete Varianten.

1.2 Dokument Historie und Status

Dokument-Status	Datum der Änderung	Version	Bearbeiter	Kommentar
Erstellung	1.10.2021	5.0.0	Cavallin	
Freigegeben	15.10.2021	5.0.10	Woisetschläger	
	15.11.2021	5.0.11	Woisetschläger	Aufnahme von ICMP/UDP in Kapitel 8
	31.01.2022	5.0.12	Cavallin / Steiner	Korrektur FULL-NAT Adressen Kapitel 3.4
	01.02.2022	5.0.13	Cavallin	ocsp.ecard.sozialversicherung.at und Freischaltelisten
	28.02.2022	5.0.14	Cavallin / Steiner	Überarbeitung hinsichtlich OCSP und Freischaltelisten, zusätzliches Praxisbeispiel Kap. 6.7, Festlegung der lokalen NW-Bereiche für Apotheken
	08.06.2022	5.0.15	Cavallin	RIP-Routing Klarstellung, Netzwerweiterung
	31.01.2023	5.0.16	Klimek	Hinweis: Prüfung der Request-IP
	18.01.2024	5.0.17	Klimek	Formatierungsverbesserungen
	06.05.2024	5.0.18	Kardinar	Ergänzung in Kapitel 5.3: DNS-Einstellungen im Browser

1.3 Kontaktinformation

Name, Organisation	Kontaktdaten	Zuständigkeit
Support	support@svc.co.at	Allgemeiner externer Partner Support für Software Entwicklung SVC

2 Grundlagen GIN (Gesundheits-Informations-Netz)

Mit der 56. ASVG-Novelle BGBl I 172 / 1999 wurde dem Hauptverband der Österreichischen Sozialversicherungsträger die Aufgabe übertragen, ein chipkartenbasiertes elektronisches Verwaltungssystem (ELSY) für die österreichische Sozialversicherung zu schaffen.
Der DVSV stellt für SV-Partner mit dem GIN ein Telekommunikationsnetz bzw. einen Telekommunikationsdienst bereit, das bzw. der die Abwicklung von SV-Anwendungen innerhalb des ELSY ermöglicht.

Das GIN setzt sich aus Sicht der Gesamtanwendung aus mehreren Teilkomponenten und vertraglichen Leistungen zusammen. Ein kurzer Überblick im nächsten Abschnitt soll die prinzipiellen Zusammenhänge informativ zeigen.

2.1 Schematischer Aufbau und Komponenten

Beim GIN handelt es sich um ein abgeschlossenes Netzwerk mit bekannten Teilnehmern. Es ist besonders gesichert und dient als Zugangsnetz für die e-card Services (SV-Anwendungen) und die zusätzlichen Mehrwertdienste (MWD, wie z.B. Befundübermittlung, Internetservices, Teleworker-Service).

Im GIN werden SV-Anwendungen und Mehrwertdienste unterstützt. Das VPN, über welches diese Dienste erreicht werden, wird in diesem Dokument als **MWD-VPN** bezeichnet.

Der Name des Netzwerkes des SV-Partners lautet **VP-LAN.**
Umgangssprachlich wird das LAN des VP auch oft Ordinations-LAN oder Apotheken-LAN genannt.

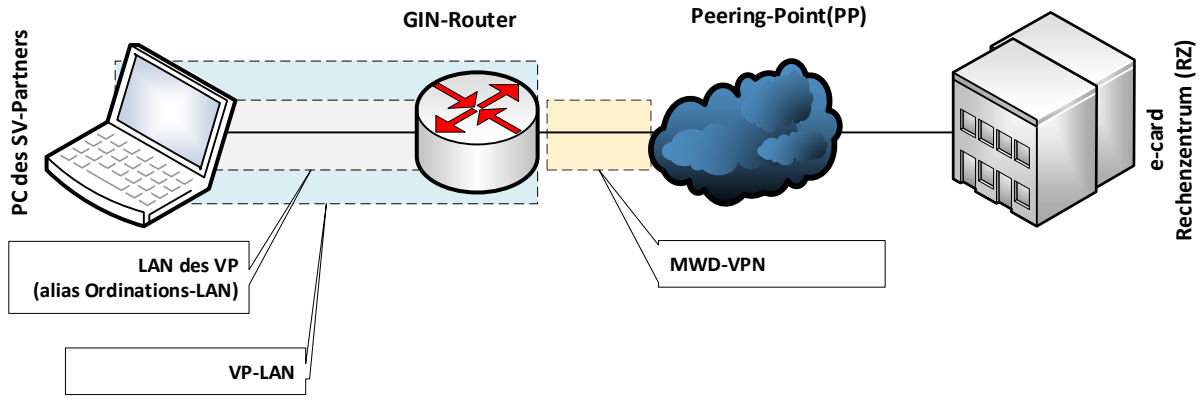

Abbildung 1: Schematische Darstellung vom GDA-LAN zum Rechenzentrum

Ab dem Übergang zum GIN-Provider sind zentrale Komponenten redundant ausgelegt.

Die hier dargestellten Strukturen dienen lediglich der Information und einem besseren Gesamtverständnis, sind aber wichtig, da sich aus dieser Implementierung auch einige technische Schlussfolgerungen und Verfahren ableiten.

Die Einrichtung PP (als Bestandteil des GINs) wurde gegründet, um allen Anbietern von Mehrwertdiensten (MWD), die sich an die Regelungen einer sicheren Datenübertragung halten, den Zugang zu ihren Kunden oder potenziellen Kunden über das GIN zu ermöglichen.

Die folgende Darstellung zeigt die Architektur und Komponenten des GINs in einer schematischen Übersicht.

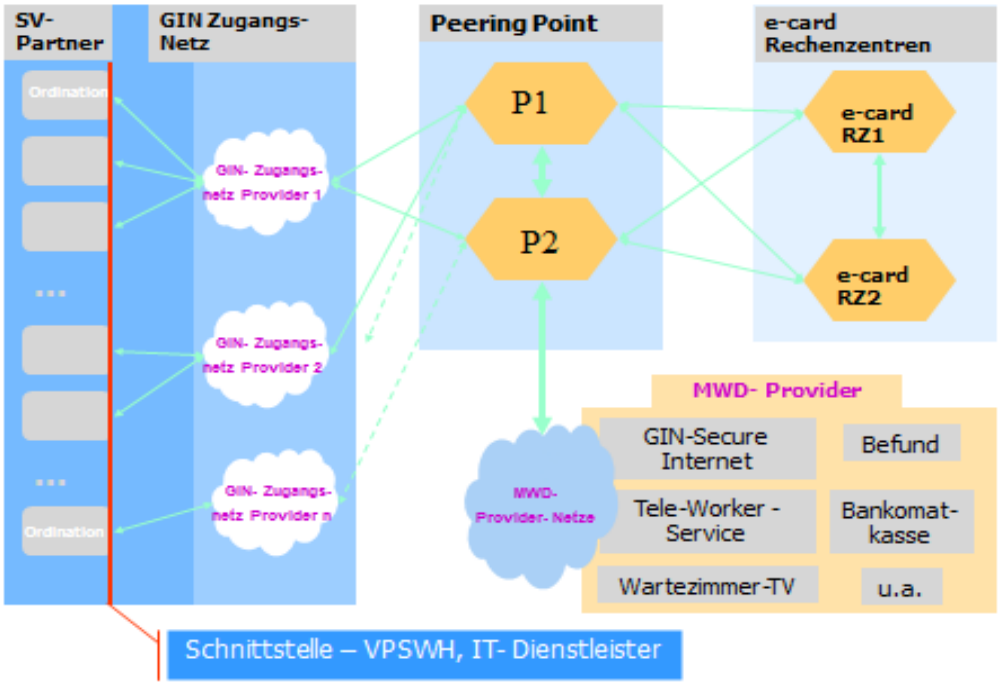

Abbildung 2: Struktur des GIN

Kurzbeschreibung und Anmerkungen:

- Die SV-Partner werden typischerweise über eine Breitband(xDSL)-Verbindung an das GIN angeschlossen. Alternativ kann diese Verbindung auch über Glasfaser oder über Mobilfunk erfolgen. Mobilfunk dient zur Überbrückung des Zeitraumes bis eine permanente, kabelgebundene Anbindung hergestellt werden kann. Es ist eine eindeutige Schnittstelle in Form des GIN-Zugangsnetz-Routers zur IT-Infrastruktur des VPs definiert.

  Siehe dazu auch **2.3 Zuständigkeiten und Schnittstelle im VP-LAN**

  Die GIN-Zugangsnetze stellen die Verbindung von der lokalen IT Infrastruktur des VPs bis zum Peering Point (PP) her. Dieser Bereich ist durch den „GIN-Zugangsnetz Providervertrag“ eindeutig geregelt (u.a. auch die Schnittstelle zur lokalen IT und die zu erbringenden Leistungen). Die GIN-Zugangsnetze sind (in sich) redundant aufgebaut und trennen das MWD-VPN strikt von anderen Netzen. Die Daten werden ebenfalls mit redundanter Auslegung an den zwei Standorten des PP übergeben.

- Die Schnittstellenkonfigurationen sind abgestimmt, standardisiert und können (bis auf die Eigenschaften des LAN-Interfaces zur VP-IT) nicht verändert werden!

- Der PP stellt die Austauschplattform für die gesamte Datenkommunikation im GIN dar. Der PP regelt und überwacht die Datenkommunikation sowohl für die Kommunikation im SV-, als auch im MWD-Bereich. Technisch ist der PP redundant ausgelegt und mit einer Reihe von technischen Sicherheitseinrichtungen ausgestattet.

- Die PP-Betriebsgesellschaft (PPG) stellt die Regeln und Sicherheitsrichtlinien für den MWD-Datenverkehr auf, überwacht diesen und regelt darüber hinaus vertragliche Beziehungen mit den am PP angeschlossenen Mehrwertdienste (MWD)-Service-Anbietern.
- Die e-card Rechenzentren sind an den PP redundant angebunden und stellen die e-card Services, ELGA Zugang und weitere SV-Anwendungen zur Verfügung.
- Für MWD-Service-Anbieter bietet der PP definierte Schnittstellen für einen gesicherten (direkten) Zugang zum GIN und damit zu allen SV-Partnern. Dieser Zugang kann (und ist bereits für bestehende MWD) ebenfalls redundant ausgelegt werden. Den Zugang regelt vertraglich die PPG. In der Darstellung sind einige dieser MWD als Services und exemplarisch auch als Produkte bzw. Anbieter aufgeführt.

Wichtig: Die Anbindung von MWD-Anbietern (technische und vertragliche Fragen) werden in diesem Dokument ausdrücklich nicht behandelt. Es folgen lediglich Informationen für den Zugriff auf solche Dienste – und die damit verbundenen technischen Rahmenbedingungen.

2.2 Die Kommunikations-Schnittstellen der GIN-Services

Im GINS werden folgende **Schnittstellen** angeboten, um Anwendungen zu nutzen:

(1) das **WEB-Interface (e-card Web-Oberfläche)** – über das sich die GINS-Applikationen per WEB-Browser bedienen lassen und

(2) das **SOAP(Simple Object Access Protocol)-Interface** (aka „SS12“) über das entsprechend angepasste VP Software direkt mit GINS und den dort erreichbaren Services kommuniziert.

(3) Die **REST Schnittstelle** (**RE**presentational **S**tate **T**ransfer) auf dem GINO (3) dient zur Kommunikation von PC/Browser bzw. VP-Software im VP-LAN (2) zum GINO (3)

2.3 Zuständigkeiten und Schnittstelle im VP-LAN

Dieser Abschnitt beschreibt die technisch-organisatorische Schnittstelle zwischen VP-Softwareherstellern (VPSWH) bzw. IT-Dienstleister (IT-DL) und dem GIN-Zugangsnetz-Provider im VP-LAN des SV-Partners.

Da bei Nichtbeachtung dieser Regelungen durchaus auch zusätzliche Kosten für den SV-Partner oder den IT-DL/VPSWH entstehen können, ist dieser Problematik besondere Aufmerksamkeit zu widmen!

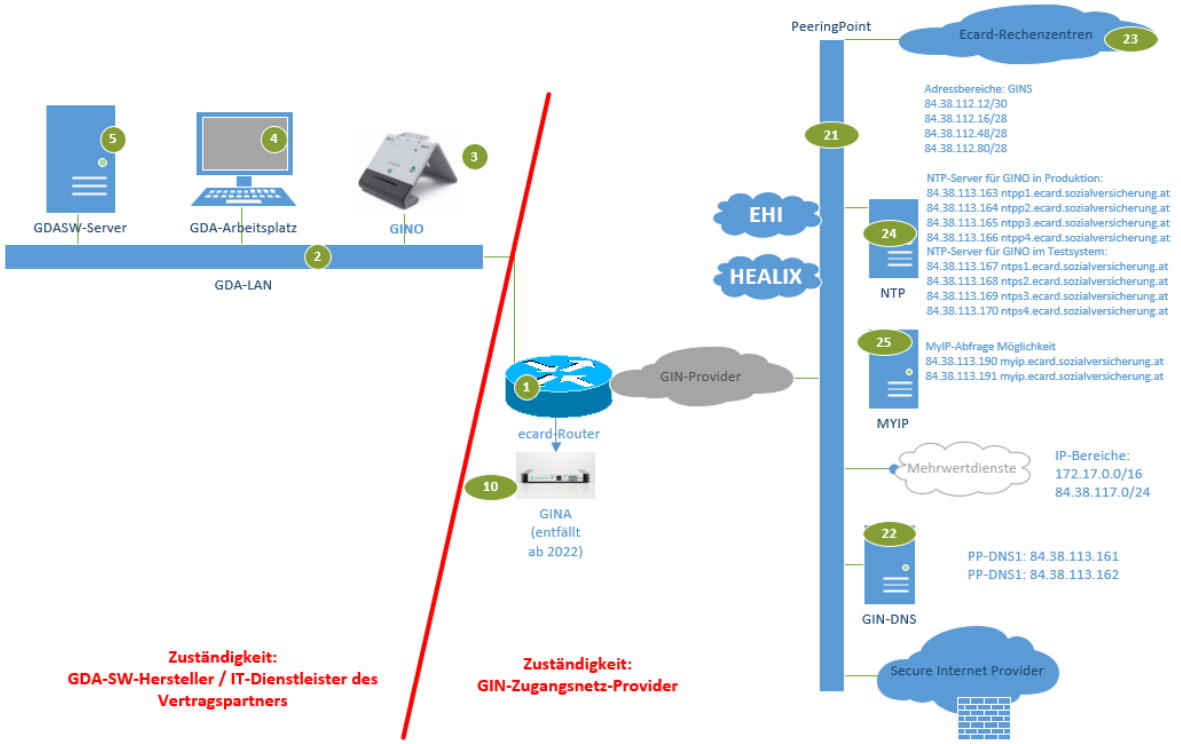

Abbildung 3: Schnittstelle im VP-LAN

2.3.1 Kurzbeschreibung der Leistungen des GIN-Zugangsnetz-Providers

- Der Provider liefert die Standardausrüstung[2] (1x Router, 1x GINO) und das Handbuch und installiert den Zugang nach seinen vertraglichen Vorgaben als Produktiv- oder VPSWH-Anschluss. Zusätzliche Komponenten wie etwa GINOs können über den Provider gemietet werden (das muss vom SV-Partner vor der Installation abgeklärt werden!).
- Alle gelieferten Geräte (insbesondere Router und GINO) liegen in der Hoheit (Installation, Konfiguration, Wartung, Betrieb) des Providers. Der GINO kann auch vom VPSWH / IT-Dienstleister konfiguriert werden.
- Die Zuständigkeit des Providers endet grundsätzlich an der Ethernet-Schnittstelle des Routers zur lokalen Infrastruktur.
  Für Neuinstallationen: **Sind vor der Installation keine Vorbereitungen des lokalen LAN erfolgt, konfiguriert der Provider an dieser Schnittstelle die Standardkonfiguration** – die DHCP-Konfiguration und Abschnitt: **3.4 Netz für das LAN des VP** (alias Ordinations-LAN) für die IP-Adressen). Zusätzlich wird zumindest ein GINO initial im VP-LAN (direkt an dem e-card-Router angeschlossen) installiert und konfiguriert.

[2] Betrifft den Zeitpunkt nach der Ablöse von GINA/LAN-CCR durch den GINO und zentrale Services (GINS)

- Der Provider ist verpflichtet, bei vorliegenden Installationsparametern, die Router-Schnittstelle zum lokalen LAN entsprechend den Vorgaben des VPSWH/IT-DL zu konfigurieren (Parameter: IP-Adresse, Maske, DHCP, RIP-Routing).
- Sonstige Änderungen von Parametern und Konfigurationen des Routers werden vom Provider **nicht durchgeführt** (bzw. sind als Abweichung vom Standard **nicht zulässig**).

2.3.2 Übergabe des Zugangs durch den Provider

Der Provider übergibt eine funktionsfähige e-card Anwendung und führt vor Ort einen einfachen Systemcheck durch.

Anmerkung: Das produktive Zentralsystem ist nicht von VPSWH-Anschlüssen erreichbar.

Service-URL für Vertragspartner:
https://services.ecard.sozialversicherung.at

Beispiel für Softwarehersteller im Test-Referenzsystem (VPSWH-Umgebung):
https://services-a.ecard-test.sozialversicherung.at

Abbildung 4: Maske aus der e-card Web-Oberfläche

Hinweis: Der Zugriff erfolgt ausschließlich über DNS-Namen. Die Verwendung der IP der zentralen Services als Zugriffsalternative (wie früher üblich) ist nicht mehr erlaubt.

Die Voraussetzung um die Services des e-card Systems und des GINS nutzen zu können, ist eine EDV-Ausstattung des Vertragspartners.

Da es die GINA nicht mehr gibt, gibt es auch keine Minimalversion mehr (mit an der GINA angeschlossenem Monitor/Tastatur).

Der Provider ist vertraglich verpflichtet, dem VP eine **funktionierende e-card Anwendung** zu übergeben. Die Funktion wird mit manuellen Test-Aufrufen getestet.

Um eine erfolgreiche Nutzung der Services im GIN (GINS) darzustellen, wird in den nächsten Abschnitten auf die technischen Randbedingungen eingegangen, die bei der Integration der e-card in dem lokalen LAN zu beachten sind.

2.4 Grundlagen der Kommunikation im GIN

Dieser Abschnitt gibt einen Überblick zu den Kommunikationsbeziehungen und Datenströmen im GIN. Daraus ergeben sich auch Implikationen für die Konfiguration in der lokalen IT, insbesondere bei individuellen Anpassungen.

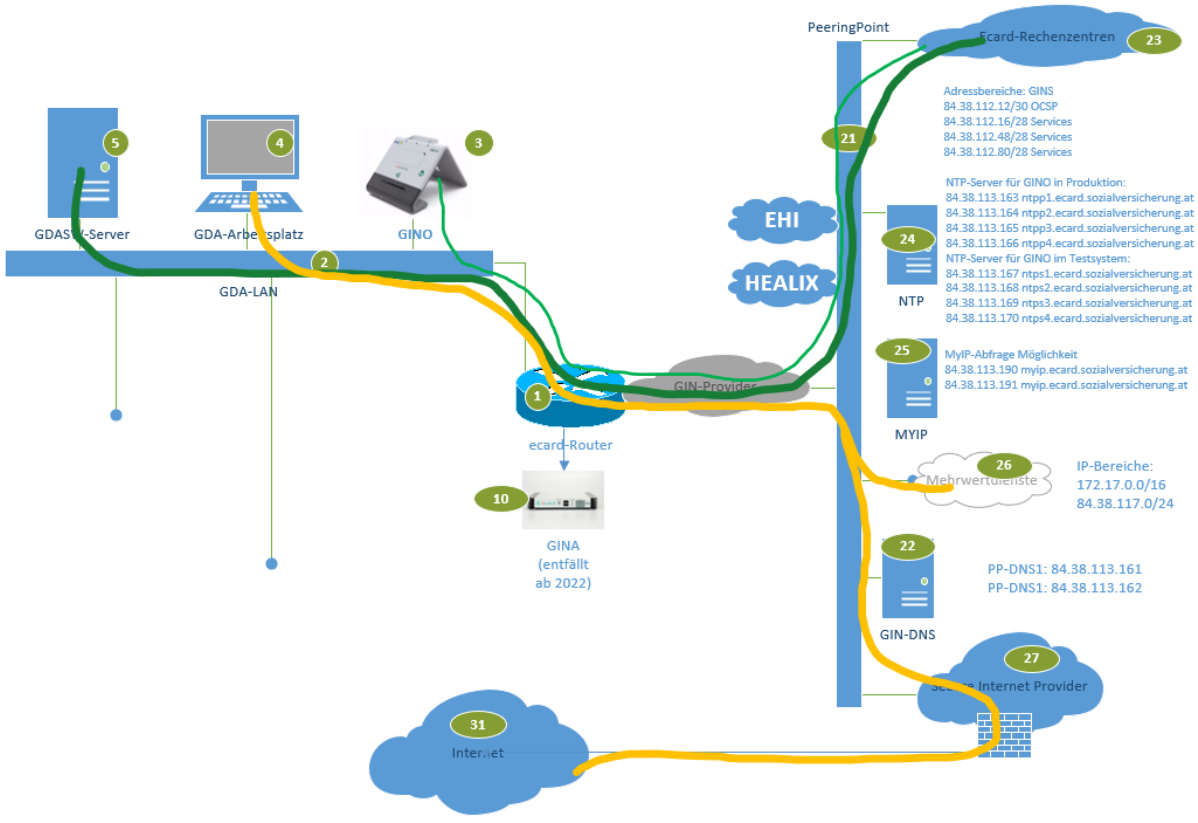

Abbildung 5: Kommunikation im GIN

Kommunikation mit SV-Anwendungen

(1) Jede Kommunikation wird vom Endgerät in dem lokalen LAN (z.B. PC (4) mit Browser oder VPSW (5)) initiiert.

(2) Für SV-Anwendungen kommuniziert das Endgerät direkt mit den Services (GINS), die durch den Router (1) via GIN-Provider und Peering Point (21) erreichbar sind.

(3) Auch der GINO (3) kommuniziert für unterstützende Services (Card Reader Service (CRS)), Softwareupdates und Wartungszwecke mit den Services im e-card-RZ (23).

(4) Der Peering Point (21) sichert das GIN zusätzlich ab und sorgt für eine Lastverteilung auf die e-card-Rechenzentren bzw. schaltet im Wartungs- oder Störungsfall auf die jeweilig aktiven Instanzen der e-card-Rechenzentren um. Der PP liefert auch die Namensauflösung (DNS) (22) für Ressourcen im GIN und Internet und die Zeit (gesichertes NTP) (24) für den GINO (3).

(5) Die Kommunikation mit e-card und ELGA Services wird gegenüber den Transfer-Services (z.B. Dokumentenupload) und Mehrwertdiensten bevorzugt transportiert (QoS).

Kommunikation mit MWD-Anwendungen (wie Befundübermittelung, Internet etc.)

(1) Der PC erreicht das MWD-VPN und damit die MWD (26) über den Router (1). Im Router erfolgt eine „Network Address Translation“ (auch „hide-NAT“ genannt) auf eine feste (und für jeden GIN-Anschluss einmalige, identifizierbare) IP-Adresse.

(2) Über das GIN werden die am PP angeschlossenen MWD erreicht. Darüber hinaus löst der DNS-Server des MWD-VPN auch alle **Internetadressen** auf.

(3) MWD-Service-Anbieter schließen mit der PPG einen Zugangsvertrag ab, der alle technischen und kommerziellen Randbedingungen regelt. Dieser Aspekt des GIN ist nicht Bestandteil dieses Dokumentes.

(4) Ein besonderer MWD ist der Internetzugang. Über den PP können damit alle SV-Partner auch einen **gesicherten Internet**-Zugang (27) sowie entsprechende Services wie E-Mail, VPN, Teleworking etc. abonnieren.

Wichtig: Unabhängig von der GIN-Zugangsnetzinstallation kann jeder SV-Partner unter den angeschlossenen Internet-Providern frei wählen. Einen entsprechenden Vertrag kann der VP direkt mit dem Internet-Provider abschließen.

2.5 Frei erreichbare Portale im GIN

Einige definierte Portale sind im GIN auch ohne MWD Internet erreichbar. Dazu zählen die Homepage der ÖÄK und Seiten der SV.

2.6 Sicherheitsaspekte (informell)

Die nächsten Abschnitte dienen dazu, die wichtigsten Aspekte aus Sicht des SV-Partners prinzipiell zu erläutern, und dem IT-DL/VPSWH fachlich richtige und gegebenenfalls auch nachprüfbare Argumente für die Beratung seiner Kunden zu vermitteln.

2.6.1 Sicherheit der Kommunikations-Wege

Der Zugang für die lokale IT zum GIN wird über den Providerrouter hergestellt. Im Gegensatz zu typischen (privaten) Breitband (ADSL) Anschlüssen ist der Router aber nicht mit dem **Internet** verbunden, sondern terminiert in einem geschlossenen, gegen alle sonstigen Datenverbindungen des Providers abgeschotteten Netz. Dies schützt den Anschluss gegen intelligente Angriffe, aber auch gegen eine Überlastung durch DDoS-Attacken.

Einzelne MWD (wie z.B. Wartezimmerfernsehen) benötigen eine direkte Verbindung ins lokale Netzwerk des VPs zu den speziell für dieses Service lokal aufgestellten Hardware-Komponenten. Nur diese Dienste haben die Möglichkeit von extern (über den Peering Point) eine Verbindung ins lokale Netzwerk aufzubauen. Dafür sind im lokalen Netzwerk besondere IPs reserviert (MWD-IP). Nur diese IPs können von den zertifizierten, angemeldeten MWD erreicht werden.

2.6.2 Sicherheit des Zugangsrouters und des GINO

Der GIN-Zugangsnetz Router ist der Verbindungspunkt zum Netzwerk des VPs.

Seine Konfiguration und Sicherheitsrichtlinien sorgen für zusätzliche Sicherheit in der Kommunikation mit den e-card und ELGA Services oder gegebenenfalls auch mit Mehrwertdiensten.

Beschreibung / Information:

(1) Der PC kommuniziert über den Router (auch GIN Router genannt).

(2) Endgeräte können mit den Services (e-card, ELGA, MWD) direkt kommunizieren.

(3) Der GINO[3] kann mit dem e-card Rechenzentrum kommunizieren; es gibt keinen Weg aus dem e-card-Rechenzentrum in das Netz des VPs. Der GINO selbst muss aktiv die Verbindung aufbauen um eine Fernwartung zu ermöglichen (siehe auch: **7 Firewall transparent (VP-LAN)** für Details).

Alle hier dargestellten Mechanismen dienen dem Schutz der Teilnehmer von Angriffen und unerwünschter Kommunikation.

2.6.3 Verschlüsselung der Daten

Alle Daten zwischen VP und den e-card/ELGA Services werden ausschließlich über eine verschlüsselte https-Verbindung übertragen. Alle Daten, die zwischen dem VP und dem e-card-Rechenzentrum ausgetauscht werden, sind daher END-TO-END verschlüsselt. Um die verschlüsselte https-Verbindung sauber aufzubauen und prüfen zu können, benötigen Browser und die Produkte der VP-Software die

[3] Hinweis: Wenn die Kommunikation des GINO zum Rechenzentrum nicht möglich ist, kann der betroffene GINO nicht über die e-card Web-Oberfläche verwendet werden und auch andere Funktionalitäten können dadurch erheblich eingeschränkt werden (z.B. Verwendung in VPSW).

entsprechenden SSL-Root-Zertifikate im Betriebssystem und im Browser installiert. Dies Zertifikate und Anleitungen dazu finden Sie hier:
https://www.chipkarte.at/zertifikate

Eine Liste der im e-card System unterstützten Browser und Betriebssysteme finden Sie passend zum aktuellen Release unter folgenden Links:

- für e-card Anwendungen (eCS)
  https://www.chipkarte.at/ecs-browser
- für ELGA
  https://www.chipkarte.at/elga-browser

Ausnahmen von verschlüsselter Kommunikation sind:

1. Teile des bis zum Rollout des GINO in Betrieb befindlichen CCS (Connectivity Check Service). Dieses nutzt auch http als Transportmittel um die Vorbereitungsarbeiten im VP-LAN zu unterstützen.
2. Der Erstkontakt eines neuen GINO mit dem Rechenzentrum (um eventuell lange gelagerte Ersatzgeräte mit folglich möglicherweise veralteter Software sicher in Betrieb nehmen zu können). Es erfolgt keine Übertragung von Karten- oder Gesundheitsdaten durch den GINO in das Rechenzentrum.
3. Die Kommunikation mit dem OCSP Service.

2.6.4 Prüfung der Anschluss- bzw. Request-IP-Adresse

Der Request des Clients an das e-card System muss von der gleichen IP-Adresse erfolgen, wie jene, mit der der GINO mit dem e-card System kommuniziert. (GIN, eHI-NET, HEALIX oder CNSV).
Bei einem Aufruf (Request) überprüft das e-card System die Request-IP-Adresse. Stimmt diese nicht mit der zugewiesenen Anschluss-IP-Adresse überein, wird der Request abgelehnt.
Hinweis: Bitte vermeiden Sie den für spezielle Anwendungsfälle reservierten FULL-NAT IP-Bereich! (Siehe Netz für das LAN des VP (alias Ordinations-LAN).)

3 IP-Adressvergabe und Schema für das Netzwerk des VPs

Die im Folgenden gezeigten Netze und IP-Adressen sind nur dann im VP-LAN wichtig, wenn nicht alle Geräte den e-card-Router als Default Gateway eingetragen bzw. vom e-card Router per DHCP bezogen haben oder eine Firewall zwischen VP-LAN und e-card Router eingebaut wird.

Die wichtigsten IP-Adressen / Interfaces für IT-DL und VPSWH sind in dieser Abbildung (rot) gekennzeichnet.

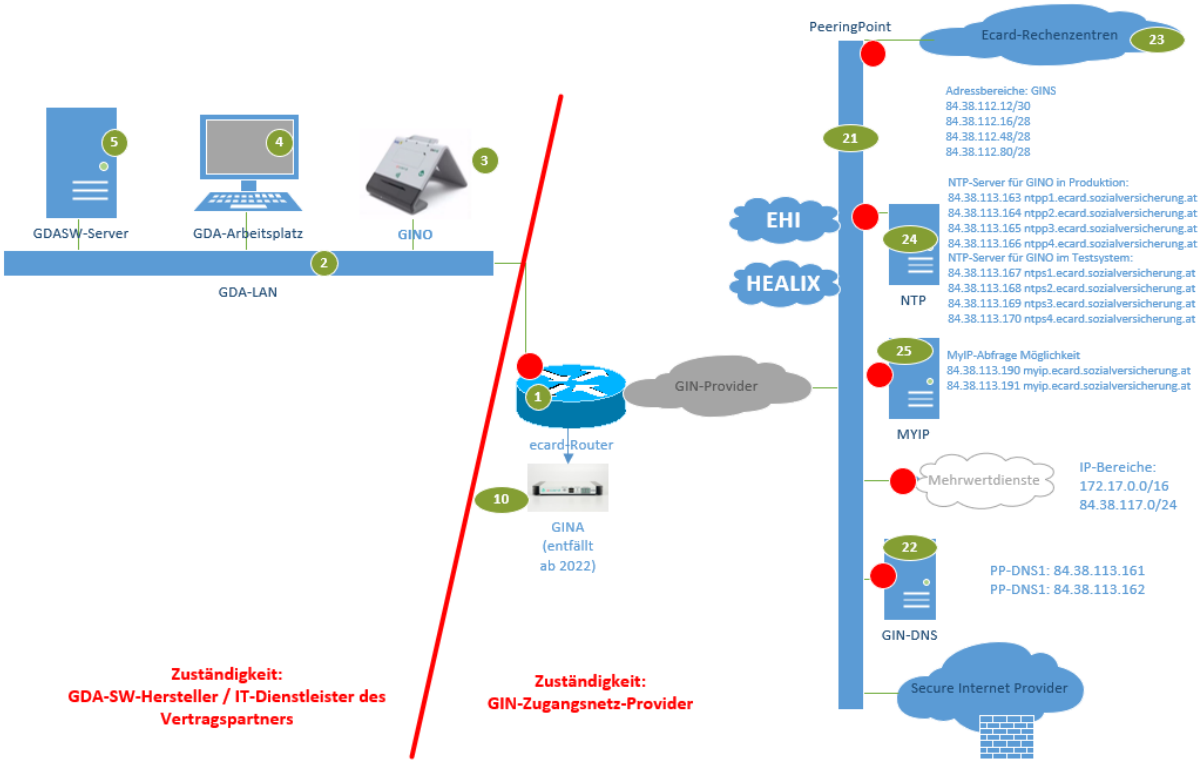

Abbildung 6: Wichtige IP-Adressen im VP-LAN

3.1 Adresszuordnung für den VP

Für jeden VP steht jeweils das MWD-VPN (**MWD**-Adressbereich) zur Anbindung an den PP zur Verfügung. Dazu kommt das **LAN-Netz** (VP-LAN) des VPs selbst.
Der SV-Adressbereich[4] bildet die Berechnungs-Basis für die Definition der weiteren IP-Adressen. Es existieren Sub-Netze für den GIN-Zugang pro Bundesland. Jeder VP erhält daraus ein Subnetz mit 16 IP-Adressen (/28)

	Berechnungsgrundlage (ehem. SV-VPN)	= MWD-VPN
VPSWH-Anschlüsse (bundeslandübergreifend)	10.196.0.0/16	10.226.0.0/16

[4] Der SV-Adressbereich wird langfristig betrachtet nur mehr aus administrativen Zwecken benötigt.

Apotheken (bundeslandübergreifend)	10.200.0.0/16	10.230.0.0/16
Ärzte Burgenland	10.201.0.0/16	10.231.0.0/16
Ärzte Kärnten	10.202.0.0/16	10.232.0.0/16
Ärzte Niederösterreich	10.203.0.0/16	10.233.0.0/16
Ärzte Oberösterreich	10.204.0.0/16	10.234.0.0/16
Ärzte Salzburg	10.205.0.0/16	10.235.0.0/16
Ärzte Steiermark	10.206.0.0/16	10.236.0.0/16
Ärzte Tirol	10.207.0.0/16	10.237.0.0/16
Ärzte Vorarlberg	10.208.0.0/16	10.238.0.0/16
Ärzte Wien	10.209.0.0/16	10.239.0.0/16

3.2 SV-Adressbereich

Basis Netz vom VP-LAN:	**10. 201. 0. 0 /28**	**255.255.255.240**

Anmerkungen:

- Für die Konfiguration des Routings im VP-LAN war dieses Netz als statische Route in den gegebenenfalls schon vorhandenen Routern einzutragen. Durch den Entfall der GINA wird dieser Eintrag künftig nicht mehr benötigt. Aus administrativen Gründen wird dieser Netzbereich weiterhin als Berechnungsgrundlage für die IP-Vergabe verwendet. Siehe dazu auch Abschnitt: **6 Routing im Netzwerk des VP**

3.3 MWD-Adressbereich

Über dieses Netz (MWD-VPN) wird der gesamte Datenverkehr zum PP abgewickelt.

Basis-Netz MWD - VPN	**10**	**.**	**231**	**.**	**0**	**.**	**0**	**/28**	**255.255.255.240**
NAT–Adresse , MWD	**10**	**.**	**231**	**.**	**0**	**.**	**1**	**/28**	**NAT-IP (hide-NAT) für Kommunikation mit GINS und MWD „Anschluss-IP“**
NAT–Adresse , "Full NAT1"	**10**	**.**	**231**	**.**	**0**	**.**	**2**	**/28**	**für spezielle Endgeräte mit 1:1 NAT, Host-IP im VP-LAN: .221**
NAT–Adresse , "Full NAT2"	**10**	**.**	**231**	**.**	**0**	**.**	**3**	**/28**	**für spezielle Endgeräte mit 1:1 NAT, Host-IP im VP-LAN: .222**
NAT–Adresse , "Full NAT3"	**10**	**.**	**231**	**.**	**0**	**.**	**4**	**/28**	**für spezielle Endgeräte mit 1:1 NAT, Host-IP im VP-LAN: .223**
NAT–Adresse , "Full NAT4"	**10**	**.**	**231**	**.**	**0**	**.**	**5**	**/28**	**für spezielle Endgeräte mit 1:1 NAT, Host-IP im VP-LAN: .224**
NAT–Adresse , "Full NAT5"	**10**	**.**	**231**	**.**	**0**	**.**	**6**	**/28**	**für spezielle Endgeräte mit 1:1 NAT, Host-IP im VP-LAN: .225**
NAT–Adresse , "Full NAT6"	**10**	**.**	**231**	**.**	**0**	**.**	**7**	**/28**	**für spezielle Endgeräte mit 1:1 NAT, Host-IP im VP-LAN: .226**
Reserve	**10**	**.**	**231**	**.**	**0**	**.**	**8**	**/28**	**Reserve**
Reserve	**10**	**.**	**231**	**.**	**0**	**.**	**9**	**/28**	**Reserve**
Reserve	**10**	**.**	**231**	**.**	**0**	**.**	**10**	**/28**	**Reserve**
Reserve	**10**	**.**	**231**	**.**	**0**	**.**	**11**	**/28**	**Reserve**

GIN-Provider MWD-VPN	10	.	231	.	0	.	12	/28	Linknetz /32
GIN-Provider MWD-VPN	10	.	231	.	0	.	13	/28	Provider
GIN-Provider MWD-VPN	10	.	231	.	0	.	14	/28	e-card-Router
GIN-Provider MWD-VPN	10	.	231	.	0	.	15	/28	Linknetz Broadcast

Anmerkungen:

- Vom SV-Adressbereich lässt sich (Addition von 30 im 2. Oktett) der MWD-Adressbereich ableiten.
- Für alle MWD (auch Internet) kann das LAN des VPs so eindeutig zugeordnet werden. Ein Konflikt mit dem LAN(-Adressen) beim VP entsteht in der Regel nicht.

3.4 Netz für das LAN des VP (alias Ordinations-LAN)

In der Standard-Konfiguration (so wie sie von den GIN-Zugangsnetz Providern installiert wird – wenn nicht vorher anders abgestimmt) wird die hier gezeigte Implementierung des LAN ausgeführt.

LAN des VP:	192	.	168	.	1	.	0	/24	255.255.255.0
DHCP – Server (auf dem Router)	192	.	168	.	1	.	1	bis 150	DHCP Adressen
Statischer Bereich	192	.	168	.	1	.	151	bis 199	für statische IP Adressvergabe im LAN des VPs
Reservierter Bereich	192	.	168	.	1	.	200	bis 220	reserviert
Full-NAT Bereich	192	.	168	.	1	.	221	bis 226	„Full-NAT“ Bereich
Reservierter Bereich	192	.	168	.	1	.	227	bis 229	reserviert
Provider-Geräte	192	.	168	.	1	.	230	bis 249	Bankomat-Terminals, statischer GINO
Netzwerk-Geräte	192	.	168	.	1	.	250	bis 253	z.B. Managed Switches, weitere Router/FWs
Router IP	192	.	168	.	1	.	254		GIN-Router „e-card Router”

Anmerkungen:

- Der Router erhält immer die .254 als IP-Adresse.
- Im Bereich von 1 bis 150 vergibt der DHCP-Server auf dem Router IP-Adressen für das LAN des VP.
- Der „statische Bereich“ steht dem IT-DL / VPSWH zur festen IP-Adressvergabe im LAN des VP zur Verfügung (Server, Router, Drucker, gegebenenfalls auch PCs).
- Der Bereich ab 200 war reserviert für besondere Verwendungen. Die Praxis hat gezeigt, dass viele LAN-CCRs statisch im Bereich über 200 existieren. Daher wird der Bereich 230 bis 249 als möglicher Bereich für GINOs dokumentiert.
- Viele dieser „Regelungen“ haben keinen funktionellen, technischen Grund, sondern sollen allen Mitwirkenden ein geordnetes Arbeiten ermöglichen.
- **Wichtig zu beachten** ist der „Full-NAT“ Bereich. Requests von Client-PCs oder Kartenlesern, deren IP-Adresse auf 221 - 226 endet, kommen im e-card System

nicht mit der "Anschluss"-IP an, sondern mit einer abweichenden Adresse.
(Hierbei ist nur das letzte Oktett der IP-Adresse ausschlaggebend.
Beispiel: 192.168.1.221 wäre ebenso problematisch, wie 10.127.1.226.)
Siehe auch: Prüfung der Anschluss bzw. Request IP-Adresse

3.5 Eigenes lokales IP Netz

Bei vorhandener IP-Infrastruktur (statisch oder auch mit eigenem DHCP-Server) bzw. nur schwer umzustellenden IP-Netz auf die im Abschnitt: **3.4 Netz für das LAN des VP (alias Ordinations-LAN)** angegebene Konfiguration sind folgende Sachverhalte zu berücksichtigen:

Netze, die im VP-LAN **nicht** verwendet werden können:

- Verwendete Netze 1 (GIN Zugangsnetze)
  - Arzt: 10.128.0.0 - 10.255.255.255
  - Apotheke[5]: 10.128.0.0 - 10.255.255.255
- Verwendete Netze 2: 172.16.0.0 - 172.31.255.255 (e-card Services)
- Offizielle Netze (nicht im RFC-1918 definiert)

Übergabeparameter an GIN-Zugangsnetz Provider: (Interface zum LAN des VP)

- IP-Adresse für den GIN-Zugangs Router
- Netzmaske
- DHCP-Server am Router ja/nein
- RIP-Routing

Bitte beachten Sie: DHCP bzw. manuelle IP-Konfiguration der PCs – insbesondere Default Gateway (siehe dazu auch Abschnitt: **3.7 DHCP Einstellungen – LAN des VP**) Über den DHCP-Server werden zum PC auch weitere wichtige Konfigurationen der Netzwerkeinstellungen am PC vorgenommen. Zum Beispiel wird/werden der/die DNS Server festgelegt. Wenn keine DHCP Konfiguration mit dem e-card DNS erfolgt, muss (zur korrekten Verwendung) auf anderem Weg im PC und im Netzwerk (am GINO) ein DNS festgelegt werden, sonst kann weder der GINO, noch der PC zum Rechenzentrum kommunizieren. (Siehe Abschnitt **5 Namensauflösung (DNS) im GIN und im VP-LAN**)

Bei Adress-/Netzkonflikten mit vorhandenen IP-Adressen im LAN des VP ist eine Umstellung der bereits vorhandenen IP-Adressen notwendig.

[5] Siehe Erläuterungen zum Netzbereich für Apotheken in Kaptiel 3.6 Freigegebene IP-Netze für das LAN des VP

3.6 Freigegebene IP-Netze für das LAN des VP

Aufgrund der globalen Netzkonfiguration (GIN, e-card-Rechenzentrum usw.) sind nicht alle „privaten“ IP-Netze für das LAN des VP verfügbar.

Wenn die „Standard“ IP-Netzwerkkonfiguration (192.168.1.0 / 24) für das VP-LAN nicht benutzt werden kann, dann ist aus den folgenden Netzen bzw. Subnetzen zu wählen:

Arzt:

Netzbereich_1:	**192.168.0.0 bis 192.168.255.255**
Netzbereich_2:	**10.0.0.0 bis 10.127.255.255**

Apotheke:

Netzbereich_1:	**192.168.0.0 bis 192.168.255.255**
Netzbereich_2:	**10.0.0.0 bis 10.127.255.255**

In der Vergangenheit wurde für Apothekennetze der erlaubte Bereich mit 10.0.0.0 bis 10.149.255.255 definiert. Allerdings fallen alle Adressen von 10.128.0.0 aufwärts in einen reservierten Bereich, der für die zukünftige Nutzung durch andere VPs / Services vorgesehen ist.
In den nächsten 3-5 Jahren (Stand 2022) ist nicht mit einer Belegung dieses Adressbereichs zu rechnen, weshalb vorläufig lokale IP-Adressen in den Apothekennetzen im Bereich von 10.128.0.0 bis 10.149.255.255 bestehen bleiben können. Dies gilt vor allem für die GINS-Netzwerkumstellung vom 14.05.2022. Es wird aber dringend empfohlen im Zuge von Wartungsarbeiten bzw. bei Neuinstallationen nur noch den NW-Bereich 10.0.0.0/9 bzw. 192.168.0.0/16 zu verwenden.

Diese Umstellung ist bis **spätestens 31.05.2027** durchzuführen.

Wenn ein Routing im LAN des VP gefordert ist, muss der GIN-Zugangs Router eine IP-Adresse aus dem Netzbereich_1 haben (siehe auch Abschnitt: **6 Routing im Netzwerk des VP**).

3.7 DHCP Einstellungen – LAN des VP

Um bei einer großen Anzahl von Installationen der e-card Anwendungen den Integrationsaufwand zu minimieren, wurde eine Standard-Konfiguration gewählt, die im Folgenden beschrieben ist.

Als typisch bzw. Standardfall der DHCP Konfiguration wird folgende Konfiguration angesehen:

- Diese Konfiguration ist die Ausgangskonfiguration für das LAN des VP bei der Auslieferung / Installation des GIN-Netzzugangs.
- Der VP besitzt (oder erhält im Rahmen der Installation) ein kleines Netzwerk, welches bisher nicht oder nur durch statische Adresseinträge in den Endgeräten gekennzeichnet ist (kein eigener DHCP-Server).

Sonderfälle, die ein Abdrehen des DHCP-Servers am e-card Router erfordern:

- Im LAN des VP wird ein komplexes Netzwerk betrieben, welches u.a. einen aktiven DHCP-Server (z.B. Server, Internet-Router oder Firewall) besitzt und durch Entscheidung des VPs bzw. seines VPSWH / IT-DL in dieser Konfiguration im Wesentlichen bestehen bleiben soll.
  → Deaktivierung des DHCP-Servers am Router
- Generell statische IP-Adressvergabe im LAN des VP gewünscht:
  → Deaktivierung des DHCP-Servers am Router

3.7.1 Übersicht zur DHCP Konfiguration im LAN des VP

Folgende Übersicht zeigt das (typische / Standard-) Szenario für die Verwendung des DHCP-Protokolls im LAN des VP. Diese Konfiguration kommt als Standard zum Einsatz, kann aber auch auf Wunsch des VPSWHs bzw. IT-DL oder durch den Provider (bei der Installation des Zuganges) ausgeschalten werden.

Kurzbeschreibung:

(1) Das Router-Interface zum LAN des VP versorgt die PCs (4) und die GINOs mit IP-Adressen und Parametern. Eine feste Zuordnung ist hier nicht erforderlich. GINOs können mit dem CRS (Card Reader Service) von der Arztsoftware gefunden werden.

(2) PCs, Notebooks etc. werden per DHCP mit den IP-Konfigurations-Parametern versorgt. Server, medizinische Geräte, Drucker etc. können, wenn gewünscht, aus dem reservierten Adressbereich auch statisch konfiguriert werden.

(3) Für GINOs ist eine DHCP-Konfiguration empfohlen, wenn auch nicht zwingend. Vorteil: Hinzufügen von GINOs ohne Vor-Ort-Einsatz möglich.

3.7.2 DHCP Parameter

Die DHCP Parameter sind fest vorgegeben. Dies betrifft auch und insbesondere das verwendete Netz. Aufgrund des Umfangs der während des Rollouts zu installierenden GIN-Zugänge, ist dies auch die einzige supportete und vom Provider zu realisierende Variante.

Anmerkung: Jede „Standard“ Konfiguration stellt immer einen Kompromiss dar; nicht für jeden VP ist dies auch ein guter. Siehe daher auch Abschnitt**: 3.7.3 Alternative Konfigurationen zum Standard DHCP**

Ein Eingriff in die Router Konfiguration durch den VPSWH oder IT-DL ist weder möglich, noch vorgesehen oder gestattet!

Für die Standard-Konfiguration wird im LAN des VP

192.168.1.0 /24 (255.255.255.0)

verwendet.

Parameter	**Wert**	**Kommentar**
Network / Mask	192.168.1.0 255.255.255.0	LAN des VP
Default Router	192.168.1.**254**	IP Interface Router in VP-LAN
DNS-Server1	PP-DNS1	84.38.113.161
DNS-Server 2	PP-DNS2	84.38.113.162
Domain-Name	**ginalan.at**	Lokaler DNS Domain Name
Lease Time	**60 Tage**	
Max leases	**150**	Bereich 151-199 frei für statische (ohne DHCP) Adressvergabe im LAN des VP (PCs, medizinische Geräte, Drucker, etc.)

Anmerkungen:

- Aus diesem Pool bedienen sich sowohl die PCs des VP als auch GINOs.
- Ein kurzzeitiger Ausfall des LAN des VP darf nicht zur Neuzuordnung von IP-Adressen insbesondere der GINOs führen. Der Provider stellt sicher dass der Router nach einem Stromausfall oder Neustart die vorher vergebenen Leases kennt. Wenn der Router keinen permanenten Speicher für die Leases hat muss dieser die DHCP-Datenbank am Peeringpoint abspeichern und bei Bedarf von dort laden. (Providerdokumentation)
- Der nicht für den Pool konfigurierte IP-Bereich wird zum einen Teil (**201-253**) für e-card und spezielle Lösungen reserviert.

- Der restliche Bereich (**151-199**) steht im LAN des VP für statische (ohne DHCP) Adresszuordnungen für Geräte zur Verfügung und kann durch den VPSWH oder IT-DL frei verwendet werden.

Ein anderes Netz bzw. veränderte DHCP Parameter sind nicht vorgesehen. Daraus folgt auch: wenn die bestehende Netzinfrastruktur den Einsatz dieser Konfiguration nicht unterstützt (Netz, Router, Domain Name), ist der DHCP-Server auf dem Router durch den Provider zu deaktivieren. Siehe dazu auch Abschnitt: **2.3.2 Übergabe des Zugangs durch den Provider**

3.7.3 Alternative Konfigurationen zum Standard DHCP

Auch wenn die Standard-Konfiguration für die Mehrheit der VP anwendbar ist, bleiben doch eine Reihe von individuellen Implementierungen (besonders größere LANs mit Servern und eigenen Netzwerkdiensten wie DNS, DHCP etc.) bestehen.

3.7.4 DHCP im LAN des VP nicht gewünscht oder nicht möglich

Falls DHCP im LAN des VP nicht gewünscht ist oder nicht unterstützt werden kann, ist folgende Vorgehensweise möglich:

…bei Nutzung des 192.168.1.0 Netzes:

- Router DHCP dennoch aktiv lassen (Standard).
- Aus dem Bereich 151-199 gegebenenfalls PCs, Drucker und Server mit **IP-Adressen statisch** versorgen – dieser Bereich ist dafür aus dem DHCP-Pool ausgenommen.
- GINOs können (müssen aber nicht) ihre IP per DHCP beziehen.
- Unterstützung für Erweiterungen (z.B. Bestellung eines zusätzlichen GINO) ist einfach.
- Mobile Geräte (Notebooks) funktionieren (Plug & Play im Netz).
- Der erste DNS Server ist der PP-DNS1, der zweite PP-DNS2 (falls kein lokaler DNS)
- Falls ein lokaler DNS genutzt werden soll, muss dieser Anfragen für zumindest die Zonen ecard.sozialversicherung.at, ecard-test.sozialversicherung.at und pki.sozialversicherung.at an die PP-DNS1 und/oder PP-DNS-2 weiterleiten.
- Für die IP-Parametrisierung der PCs an die Vorgaben aus Punkt **3.7.2 DHCP Parameter** halten.

Anmerkung: Der DHCP-Service des Routers kann auf Wunsch deaktiviert werden.

3.7.5 Eigenes Netz – statisch oder mit DHCP

Ist bereits eine größere Netzwerkinstallation vorhanden (mit eigenem/anderem IP-Netz), so ist individuell zu entscheiden, ob folgende Vorgehensweisen möglich sind:

- Bei **nicht vorhandenem (lokalen) DHCP** – Umstellung des Netzes auf den „Standard“ von 192.168.1.0.
  Dabei können sowohl statische / manuelle Adressvergaben und/oder auch Adressvergaben per DHCP erfolgen.

- Bei **statischer IP-Konfiguration** der einzelnen Server und Endgeräte und dem „Zwang“ der **Beibehaltung des Netzes** muss das DHCP-Service des Routers abgeschaltet werden (durch den Provider). Die GINOs müssen in diesem Fall ebenfalls manuell (vor Ort) konfiguriert – sprich mit fester IP-Adresse – versorgt werden. Dieses Vorgehen ist bezüglich Installation und Betreuung die Variante mit dem größten Aufwand.

- Bei eigenem IP-Netz und vorhandenem DHCP-Service ist lediglich der Router (bei der Installation) mit einer reservierten (statischen) IP zu versehen. Kollidiert das Netz nicht mit denen des GIN, ist die Integration relativ einfach.

3.7.6 Ethernet-Interface und IP-Konfiguration GINO

Um eine möglichst hohe Kompatibilität zu bestehenden Ethernet Netzen zu gewährleisten, werden die LAN-CCRs mit Speed und Duplex „**auto“** als Interface-Konfiguration ausgeliefert.

Ethernet-Interface Eigenschaften:

- 10/100 (**Auslieferzustand: auto**), **manuell konfigurierbar**
- Duplex Full/half/auto (**Auslieferzustand: auto**), **manuell konfigurierbar**
- mdx-i ist vorhanden (**Auslieferzustand: ein**)
- MAC-Adresse ist an der Vendor-ID „00-0F-D5“ erkennbar.

IP-Eigenschaften:

- IP-Adresse/Maske per DHCP oder statische Konfiguration (**Auslieferzustand: DHCP**)
  - Wenn nach langer Zeit keine IP per DHCP bezogen werden konnte: Wie beim LAN-CCR: 192.168.1.2/24, NEU: Maintenance Mode zeigt IP-Adresse, Subnet Mask und Gateway am Display an, Ultima Ratio => Factory-Reset
- Default-Gateway per DHCP oder statische Konfiguration (**Auslieferzustand: DHCP**)
  - **Es sind keine zusätzlichen statischen Routing-Einträge möglich.**
- DNS: per DHCP oder statische Konfiguration (**Auslieferzustand: DHCP**), zwei Einträge möglich
- NTP: 4 Einträge, via KALVE konfigurierbar

4 GINO – Kommunikation und Konfiguration

Mit der Basisinstallation beim VP wird vom Provider zumindest ein GINO in Betrieb genommen. Dieser muss für den Supportfall direkt mit einem Ethernet-Anschluss des Routers verbunden werden. Weitere GINOs (am typischen Router stehen 4 Ports für das VP-LAN zur Verfügung) können mittels zusätzlichen Ethernet-Switches angebunden werden.

Auf den folgenden Seiten sind Screenshots des GINOs zu sehen. Aufgrund des frühen Entwicklungsstandes sind Änderungen vorbehalten.

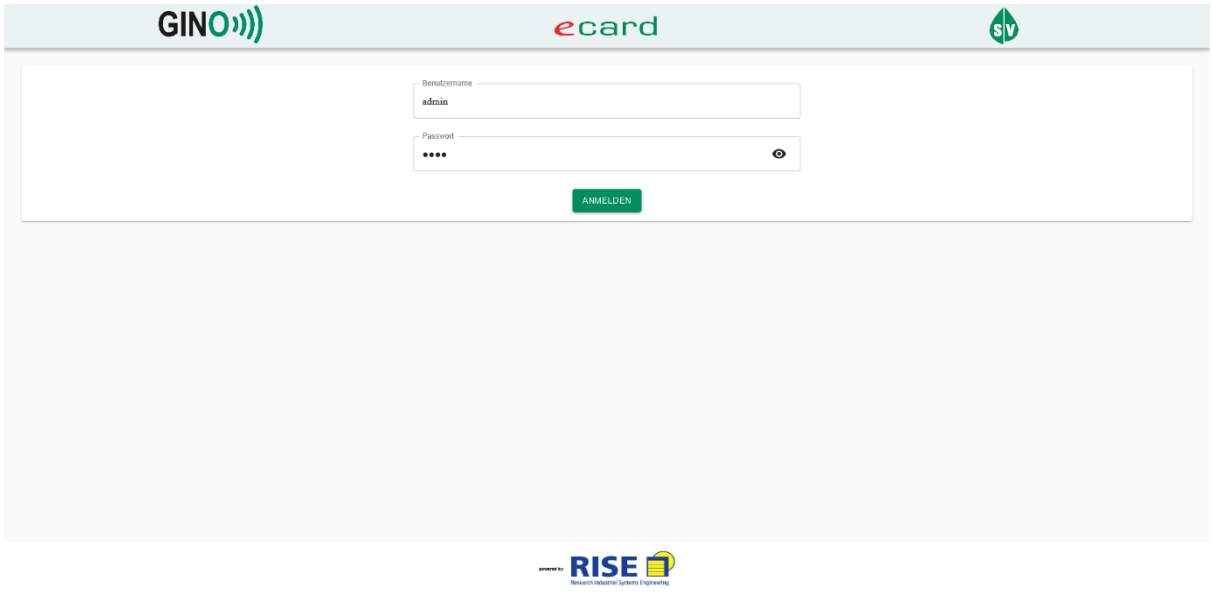

Abbildung 7: GINO User Interface – „Login“ Maske

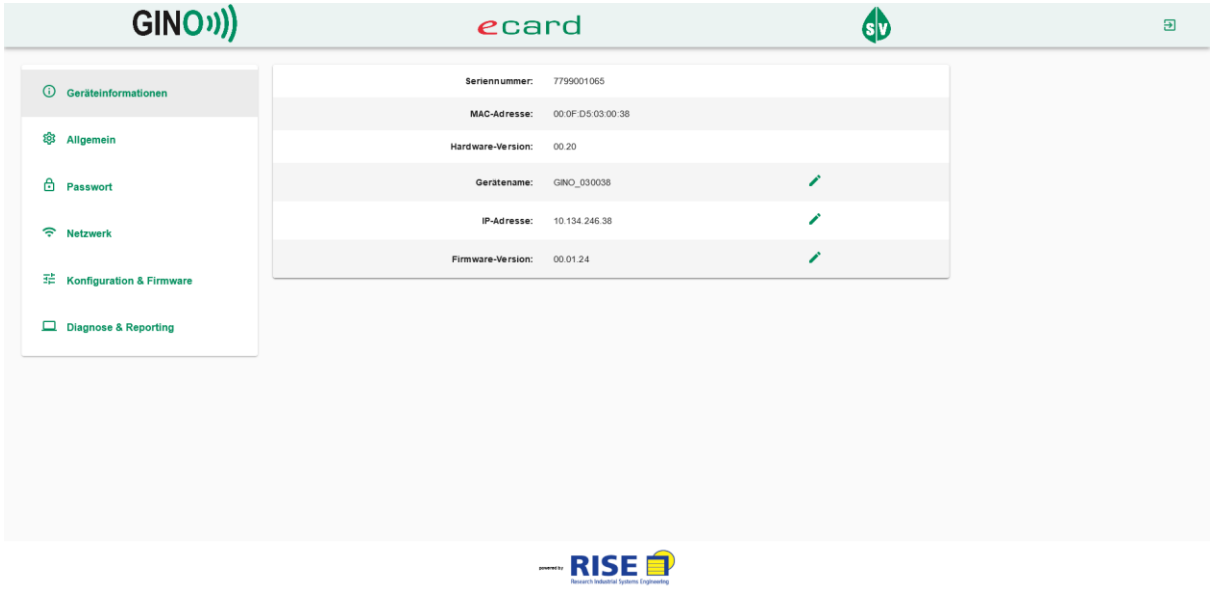

Abbildung 8: GINO User Interface – Geräteinformation

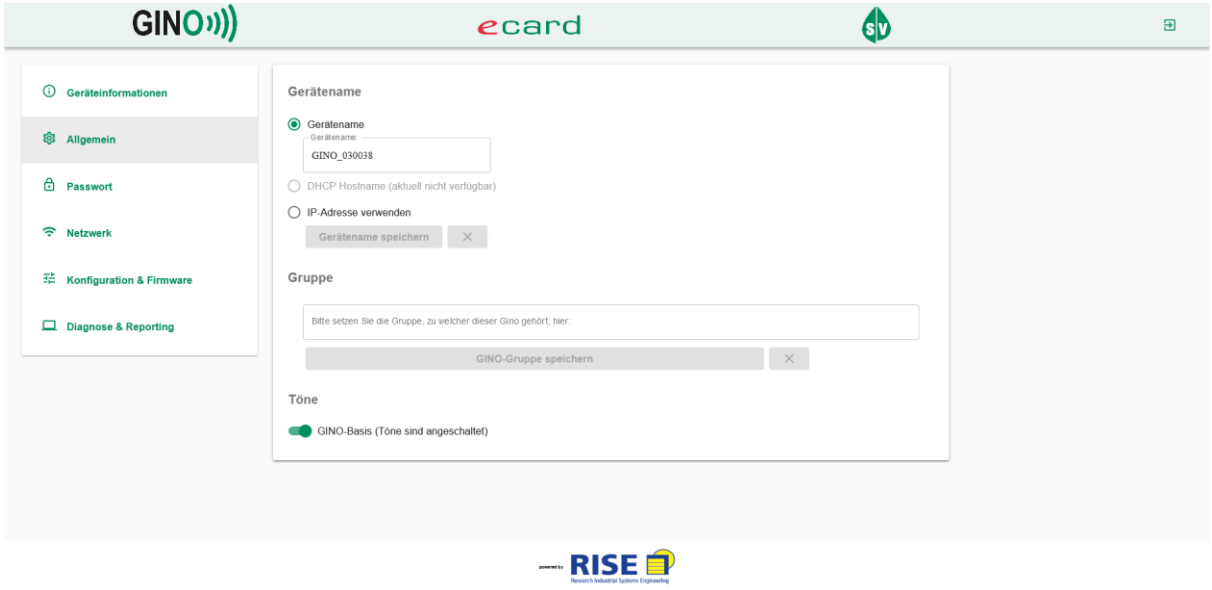

Abbildung 9: GINO User Interface – Allgemein

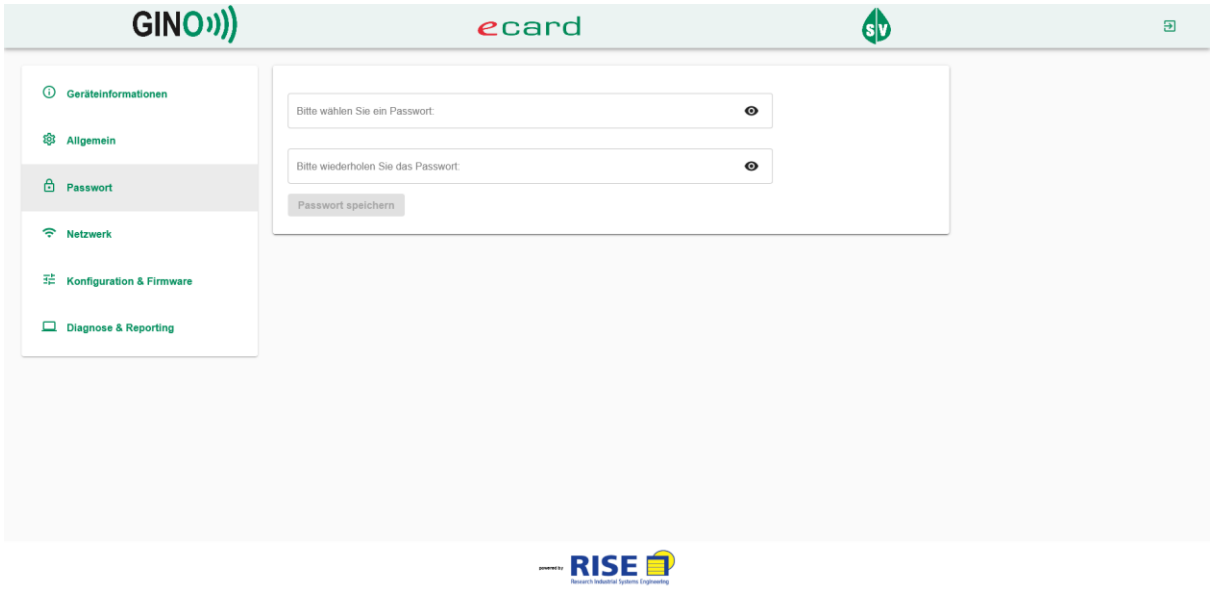

Abbildung 10: GINO User Interface – Passwort Änderung

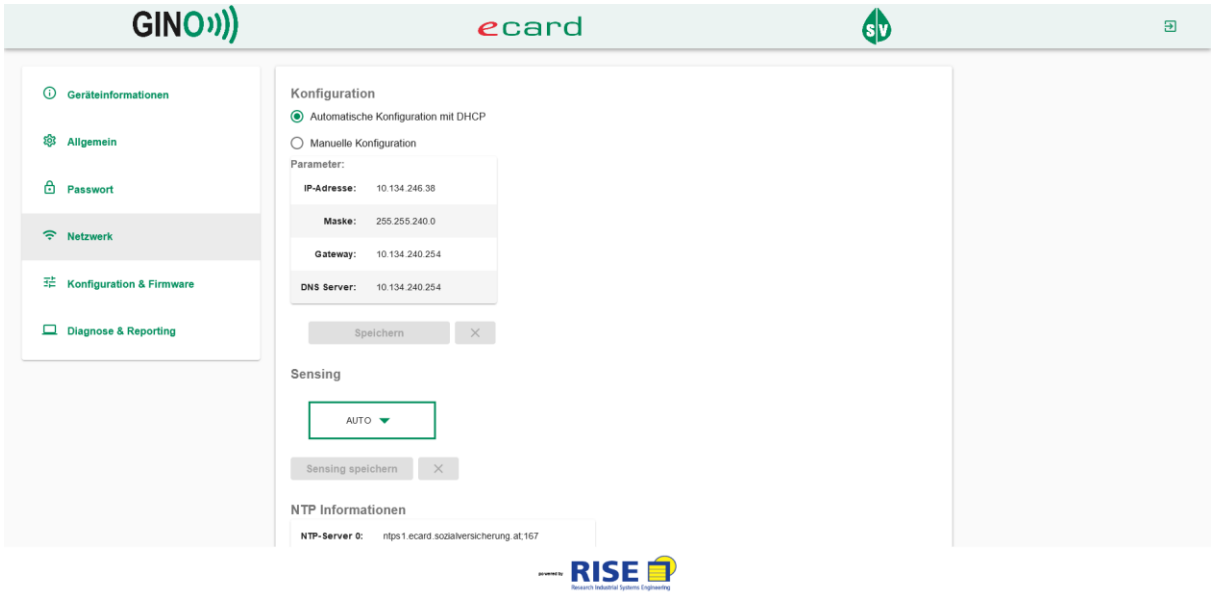

Abbildung 11: GINO User Interface – Netzwerk

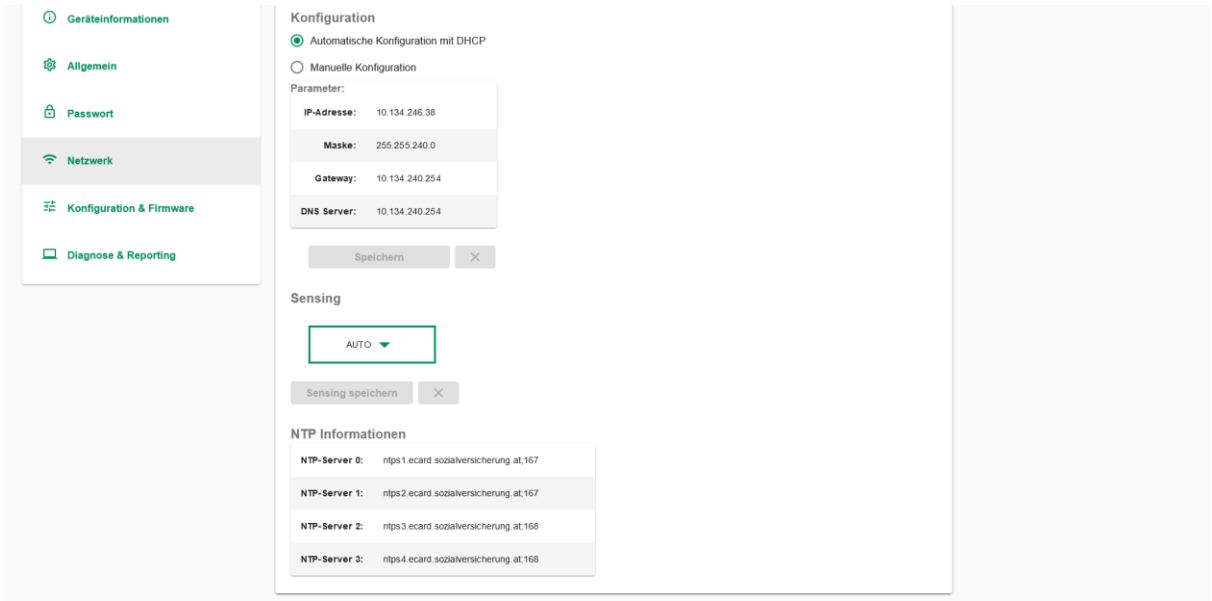

Abbildung 12: GINO User Interface – Netzwerk (NTP Einstellungen)

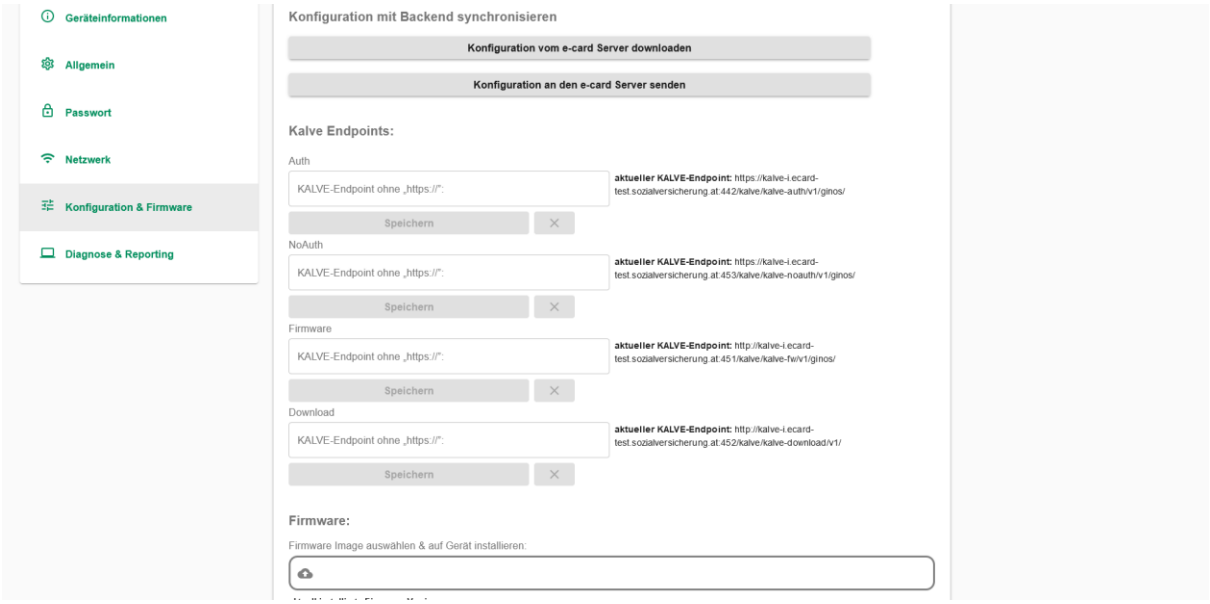

Abbildung 13: GINO User Interface – Konfiguration & Firmware 1/2

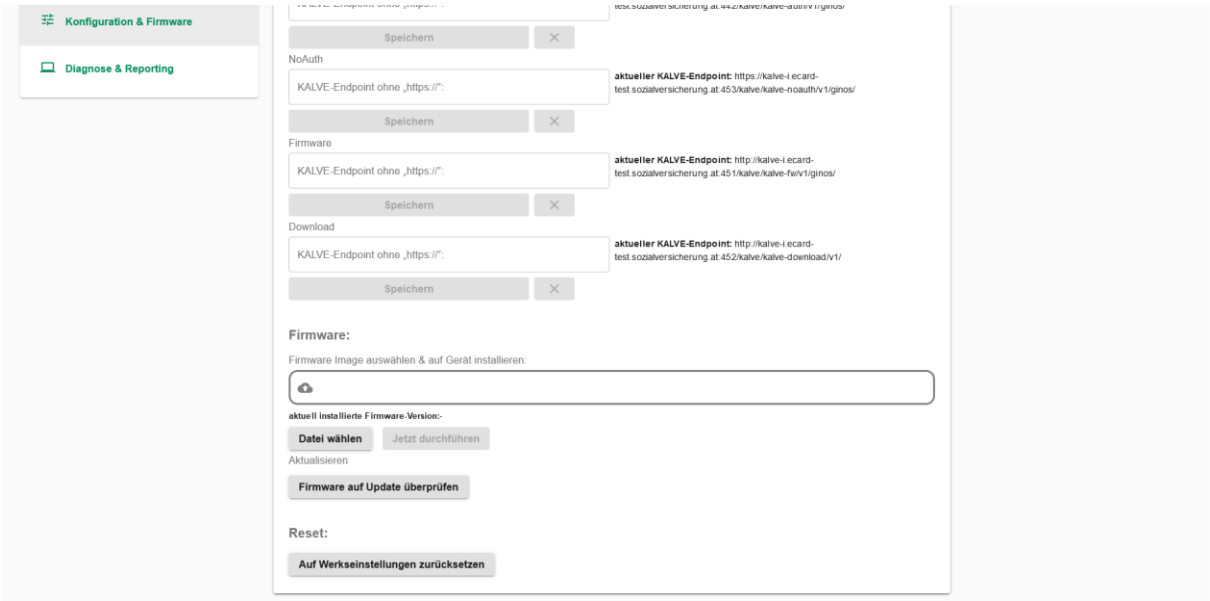

Abbildung 14: GINO User Interface – Konfiguration & Firmware 2/2

Abbildung 15: GINO User Interface – Diagnose & Reporting

5 Namensauflösung (DNS) im GIN und im VP-LAN

Einer der wesentlichen (und für die Funktion des GIN und seiner Applikationen unbedingt erforderlichen) IT-Infrastruktur-Dienste ist das DNS-Service.

5.1 DNS-Server am PeeringPoint

DNS-Services werden durch den PP bereitgestellt. Im PP sind die DNS-Services redundant ausgelegt und werden zusätzlich durch Firewalls vor Netzwerk-Attacken geschützt.

PP-DNS1: 84.38.113.161
PP-DNS2: 84.38.113.162

Folgende Zonen werden, neben weiteren, autoritativ auf den PP-DNS gehostet:

- ecard.sozialversicherung.at
- pki.sozialversicherung.at
- ecard-test.sozialversicherung.at
- sozialversicherung.at
- sozialversicherung.gv.at

Diese DNS-Server lösen alle Zonen im GINS auf und leiten unbekannte Anfragen zu Internet-DNS-Servern weiter.

5.2 DNS-Server beim VP

Typische (größere) Netzwerke bei VPs sind durchaus auch mit Server und entsprechenden Netzwerkdiensten ausgestattet. In solchen Fällen besteht dann oft auch eine adäquate Konfiguration des Netzes, in die die GINS (und damit die e-card Services) und MWD integriert werden können.
In diesen Umgebungen bietet es sich an die genannten Zonen zu den PP-DNS weiterzuleiten (siehe Kapitel 5.1).

5.3 Internet DNS für die Auflösung von Services im GIN

Ausgewählte Services der GINS werden – als Workaround, um den realen Gegebenheiten zu entsprechen – im Internet auflösbar (aber nicht via Internet erreichbar) sein. Aus Sicht der Betriebssicherheit wird die Nutzung von öffentlichen DNS für Services im GIN nicht empfohlen.[6]

[6] **Hinweis:** Einige Browser erlauben die Eintragung eines eigenen DNS für den Internet-Zugriff über den Browser bzw. haben bereits einen öffentlichen DNS als Default-DNS eingetragen. In diesem Fall kann trotz korrekter Eintragung der PP-DNS am Router bzw. Betriebssystem der Zugriff auf die e-card Web-Oberfläche über den Browser scheitern. (Siehe auch DNS-Einstellungen im Browser.)

Doppeltes Ausfalls-Risiko: Internet-Anbindung und GIN-Anbindung müssen funktionieren.
Der direkte Aufruf der Services über die IP-Adressen ist nicht möglich und nicht erlaubt.

5.4 Namensauflösung – GINA (obsolet) als DNS-Server – Folgen für die VP-Konfiguration

Die GINA stellte aus Sicht des VP den ersten DNS-Server dar. Durch den Entfall der GINA wird im Zuge des GINS/GINO Rollouts die DHCP-Konfiguration des e-card Routers so verändert, dass die beiden PP-DNS an DHCP-Clients ausgeliefert werden.
Statisch konfigurierte Geräte im VP-LAN sollen daher entsprechend korrigiert werden. Der GINO, im Falle einer statischen IP-Konfiguration, wird durch den Provider-Techniker im Zuge der Installation mit diesen beiden DNS-Servern eingerichtet werden.
Da im Zuge des GINO Rollouts keine Abhängigkeit zwischen Provider-Techniker und VPSWH/IT-DL entstehen soll, erhält der e-card Router zum Umstellungszeitpunkt eine spezielle Konfiguration, die DNS-Anfragen an die GINA-IP an die PP-DNS weiterleitet.

5.5 DNS-Forwarding durch den e-card-Router

Die GIN-Provider haben eine Konfiguration erarbeitet, welche DNS-Anfragen an die GINA-IP an einen der PP-DNS weiterleitet.
Für den Client ist dieser Vorgang transparent – es scheint der DNS-Server auf der (nicht mehr vorhandenen) GINA zu antworten.

Details zu dieser Konfiguration sind der Beilage zur Provider-Dokumentation zu entnehmen. Diese ist den GIN-Providern zugänglich.

5.6 Namensauflösung (DNS) für Mehrwertdienste

Standardmäßig werden die Ressourcen der MWD über die beiden PP-DNS aufgelöst. Durch die Harmonisierung der Systeme (Kanalzusammenlegung, Überarbeitung des DNS-Systems am PP, Entfall der GINA) besteht im Standardfall kein Unterschied zwischen der DNS-Auflösung von e-card (e-card, ELGA) und Mehrwertdiensten.

Szenario:

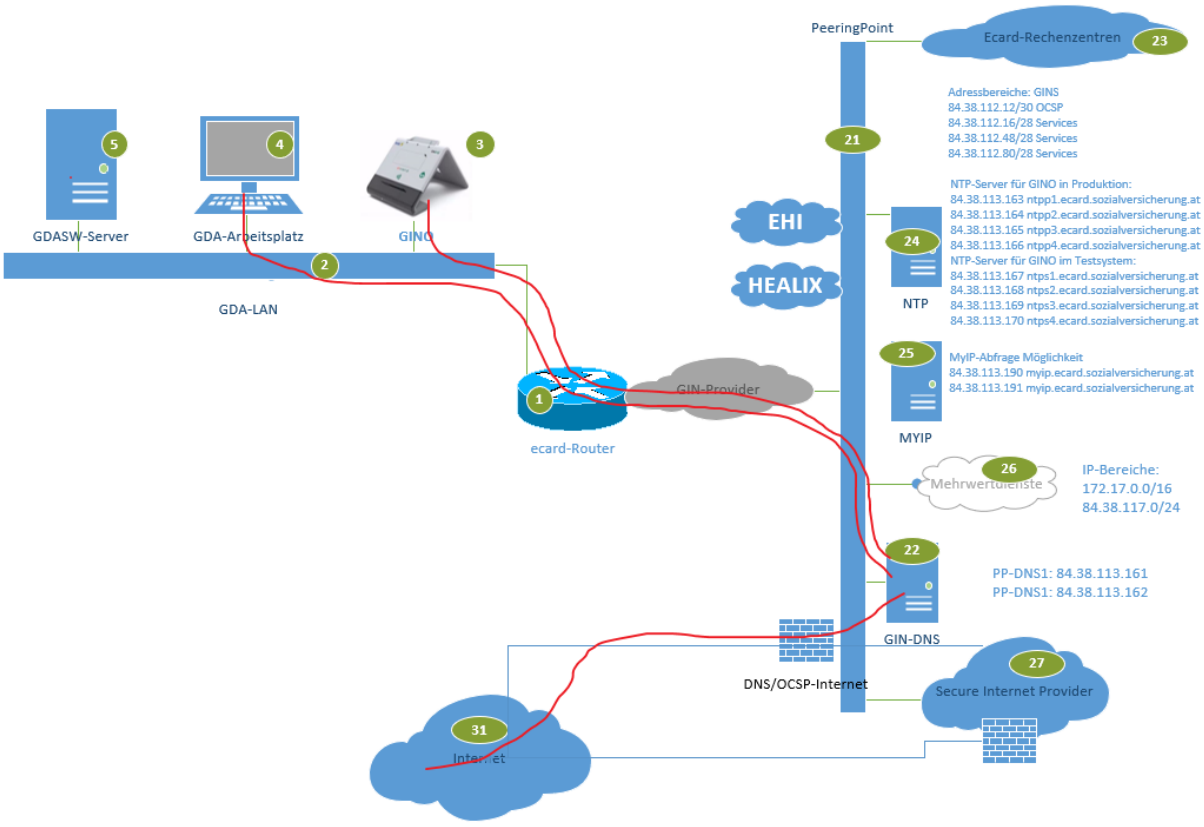

Abbildung 16: Namensauflösung für Mehrwertdienste

(1) Alle Geräte aus dem VP-LAN lösen über die PP-DNS auf.

(2) Sollte der VP einen zusätzlichen Internetanschluss haben, kann als dritter DNS der jeweilige Internet-DNS eingetragen werden. Für den unwahrscheinlichen Fall einer DNS-Störung (beider PP-DNS) am PP oder eines Leitungsausfalles der GIN-Anbindung würde diese Vorgangsweise Einschränkungen bei der Namensauflösung im GIN mit sich bringen, aber die Auflösung für das Internet aufrechterhalten.

Anmerkung: Ein IP-Stack eines PCs benutzt immer/typisch den ersten funktionsfähigen DNS-Server zur Namensauflösung. Es wird erst dann auf den zweiten Eintrag umgeschaltet, wenn der erste DNS-Server keine Antworten mehr liefert. Also beispielsweise bei einer Leitungsstörung der GIN-Anbindung.

5.7 Namensauflösung mit lokalem DNS-Server im Netzwerk des VP

Typische (größere) Netzwerke bei VPs sind durchaus auch mit Server und entsprechenden Netzwerkdiensten ausgestattet (Windows, Linux u.a.). In solchen Fällen besteht dann oft auch eine adäquate Konfiguration des Netzes, in die die GINS (und damit die e-card Services) und MWD integriert werden können.

Damit ergeben sich auch weitere Vorgehensweisen für die Integration von GINS und MWD, die auf den in vorangegangenen Abschnitten dargestellten Grundlagen und Zusammenhängen aufbauen.

5.7.1 Schaubild Namensauflösung mit lokalem DNS

Wie im Abschnitt **5.6 Namensauflösung (DNS) für Mehrwertdienste** schon erwähnt, werden die **Namen aller Services** und alle **Internet-Namen (URLs)** auch über die DNS-Server des PP aufgelöst.

Da diese DNS-Server **nur über das GIN erreichbar** sind, sind diese Server auch als „Forwarder“ für eine lokale DNS-Konfiguration zu verwenden.
Die folgende Abbildung zeigt die Zusammenhänge für eine empfohlene / mögliche Konfiguration schematisch.

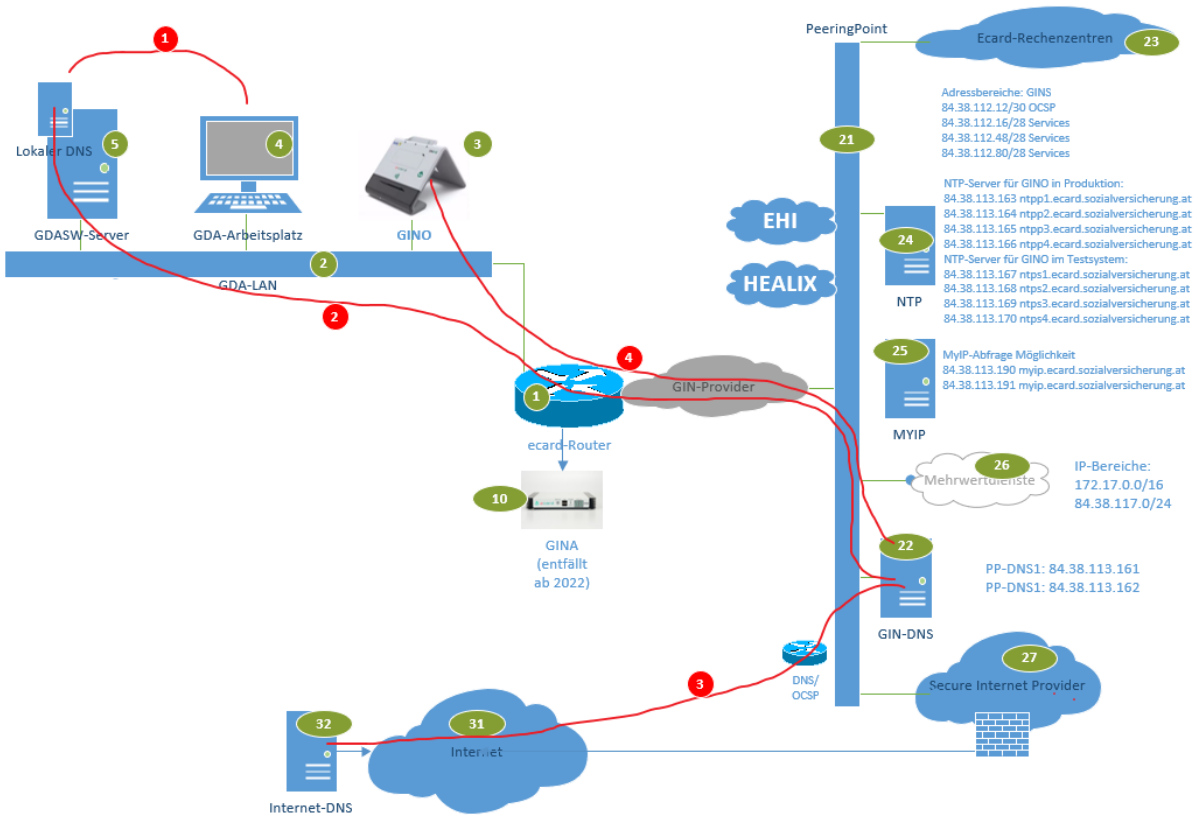

Abbildung 17: lokales DNS im Netzwerk des VP

Prinzipien und Funktion:

(1) Die PCs im VP-LAN benutzen die/den lokalen DNS-Server zur DNS-Namensauflösung.

(2) Der lokale DNS leitet Requests an den PP-DNS weiter. Der PP-DNS löst den Request auf.

(3) Abfrage in das Internet über eine abgesicherte und redundante Anbindung an das Internet – **nur für DNS.**

(4) Der GINO soll direkt zu den PP-DNS konfiguriert werden.

Hinweis:

- Das GIN bietet zwar DNS-Namensauflösung für Internet URLs – bietet standardmäßig **aber keinen Internetzugang!**
- Für einen gesicherten Internetzugang kann der SV-Partner einen Vertrag mit einem Internet-MWD-Anbieter (welcher direkt am PP angeschlossen ist; derzeit: A1, Hutchison Drei Austria, Magenta) abschließen.
- Der SV-Partner hat, unabhängig von seinem GIN-Provider, die freie Wahl aus den akkreditierten Providern. [LINK]

5.7.2 Verfügbarkeit und Zuständigkeit

Wird ein lokaler DNS-Server verwendet, liegt die Verantwortung für die ordnungsgemäße Konfiguration und den Betrieb beim VP bzw. seinen Dienstleistern.

Ein Ausfall des DNS kann direkt zum Ausfall der e-card Applikationen und der MWD (z.B. Befundübermittelung) führen.

Diese Konfiguration wird **nicht** von der e-card Serviceline (mit Diagnose und telefonischer Unterstützung) supportet, da der e-card Serviceline der individuelle Aufbau vor Ort nicht bekannt ist.

Die e-card Serviceline kann lediglich (bei bestehender Verbindung) eine Ferndiagnose des Routers, und bis zu einem gewissen Grad des GINOs durchführen. Der GINO ist nicht aktiv aus dem e-card-Rechenzentrum (RZ) erreichbar, er schreibt aber zyklisch Health-Reports an das RZ (KALVE).

5.8 Vorhandene DNS, DHCP – Dienste im Netzwerk des VP

Folgende Darstellung zeigt schematisch ein mögliches Szenario:

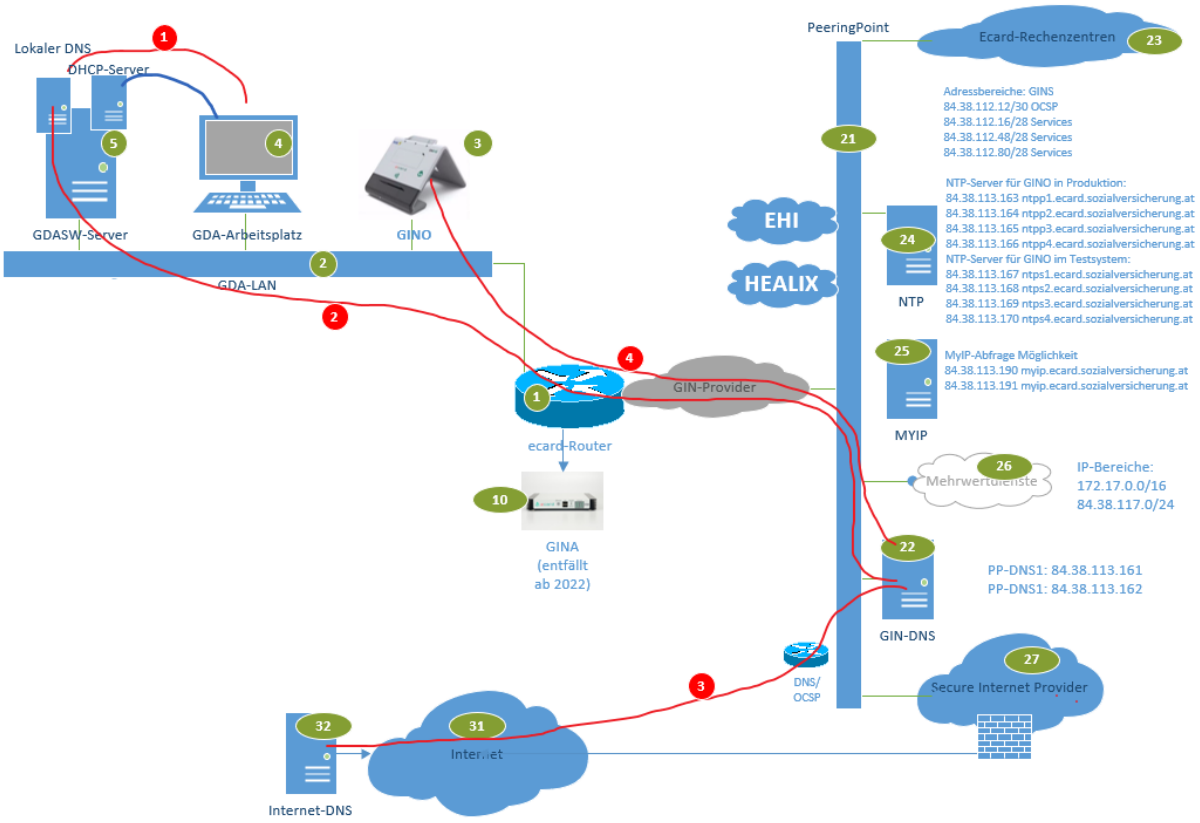

Abbildung 18: Ordination mit LAN und PCs

Beschreibung:

- Im Netzwerk des VP werden eigene DNS- und DHCP-Server verwendet.
- Der GIN-Zugangsnetz Router darf daher die Endgeräte und auch die GINOs nicht zeitgleich per DHCP mit IP-Parametern versorgen.

Vorgehensweise DHCP:

- DHCP (VP-LAN-Pool) im GIN-Zugangsnetz Router (1) deaktivieren.
- Im DHCP eine Adresse reservieren oder eine Adresse außerhalb des LAN-DHCPs für den Router verwenden – Abstimmung mit IT-DL vor Ort.
- Konfiguration des LAN-Interfaces des Routers entsprechend den lokalen IP-Netzvorgaben (IP, Mask) einrichten.
- Für die GINOs kann die IP-Konfiguration ebenfalls über den lokalen DHCP-Server erfolgen. Eine Reservierung der IP-Adressen ist vorzunehmen. Die Lease Zeit sollte mindestens 60 Tage betragen.
- Wenn der GINO **(3)** von der Verfügbarkeit der lokalen DNS und DHCP Services unabhängig sein soll, ist in dieser Situation eine statische Konfiguration des

GINOs eine gute Lösung (→ IP-Adresse außerhalb des DHCP-Pools wählen oder blockieren).

DHCP Parameter des lokalen DHCP-Servers:

- Der per DHCP an die Clients und auch die GINOs weitergegebene IP-Parameter „Default Gateway“ muss auf den GIN-Zugangsnetz Router zeigen (gegebenenfalls also eintragen oder ändern).
- **Sonderfall***:* Vorhandenes Gateway / Router im VP-LAN
  Bleibt ein vorhandener Gateway-Eintrag im DHCP-Service des LANs erhalten (zeigt also auf einen anderen als den e-card Router), sind an diesem Router die notwendigen Änderungen auszuführen, sodass die e-card Services erreicht werden.

  Siehe dazu auch Abschnitt: **6 Routing im Netzwerk des VP**

6 Routing im Netzwerk des VP

Bei größeren Installationen mit diversen Subnetzen kann es zu Konstellationen kommen, in denen die Standard-Konfiguration nicht anwendbar ist. Dies trifft besonders dann zu, wenn IP-Subnetze vorhanden sind, die über Router (auch remote) andere Teil-Standorte des VPs versorgen (der GIN-Zugangsnetz-Router ist in diesem Falle **nicht** das „Default-Gateway“).

Um dennoch den IT-DL und VPSWH vor Ort die Möglichkeit zu geben, die vorhandenen Netzkonfigurationen / Infrastruktur in diesem speziellen Fall weiter zu betreiben, wurde die nachfolgend erläuterte technische Lösung implementiert (im GINA-Router).

6.1 Support und Zuständigkeit

Die Änderungen in der Router-Konfiguration wurden so gewählt, dass sie für alle (rund 12.000) VPs anwendbar sind, und so keine lokalen Sonderkonfigurationen auf dem e-card Router entstehen, die einen effektiven Support durch die SVC bzw. die e-card Serviceline und die Provider selbst verhindern.

Die in den folgenden Abschnitten dargestellte Lösung ist ein Kompromiss zwischen den „technisch machbaren Lösungen“ und einer im Betrieb des Gesamtnetzes (GIN) durch alle Beteiligten zu „supportende“ Lösung.

Schnittstellen und Zuständigkeiten:

- Die Provider ändern in keinem Falle die Konfiguration der GIN-Zugangsnetz[7]-Router.
  (Einzige Ausnahme: Die Provider schalten auf Wunsch DHCP auf diesem Router ab und stellen eine feste IP-Adresse aus der zulässigen Range am Router ein)

- Die e-card Serviceline kann die Erreichbarkeit des Routers und die Logfiles der GINOs prüfen und gegebenenfalls die Wartung durch den Provider veranlassen. Ein aktiver Zugriff auf den GINO ist nicht möglich. Daher muss der VP eine Taste am GINO betätigen, die den GINO dazu bringt, eine Verbindung in das Rechenzentrum aufzubauen. Details zu dieser Funktion sind aktuell noch nicht fertig entwickelt und werden nachgereicht.

- **Alle Endgeräte und auch insbesondere GINOs, die sich über Routing in anderen Segmenten befinden oder remote sind, werden nicht supportet. Dafür ist der jeweilige IT-DL oder VPSWH vor Ort zuständig.**

- Wird über die e-card Serviceline eine Störungsbeseitigung angefordert, dann wird der jeweils zuständige Provider mit seinen lokal verfügbaren Technikern

[7] RIP2 sollte per Default am e-card Router aktiviert sein.

diesen Auftrag ausführen. Ist das Netzwerk des VP die Ursache für den Fehler, wird dieser Einsatz üblicherweise vom Provider kostenpflichtig verrechnet.

- Im Abschnitt: **6.6 e-card „Referenz-System“ bei Routing und Firewalls** wird auf die immer notwendige „Backup e-card Lösung“ verwiesen, welche nicht nur den Betrieb bei Ausfällen im Netzwerk des VP sicherstellt, sondern auch dafür sorgt, dass voller Support für diese Geräte von Seiten der e-card Serviceline gegeben ist.

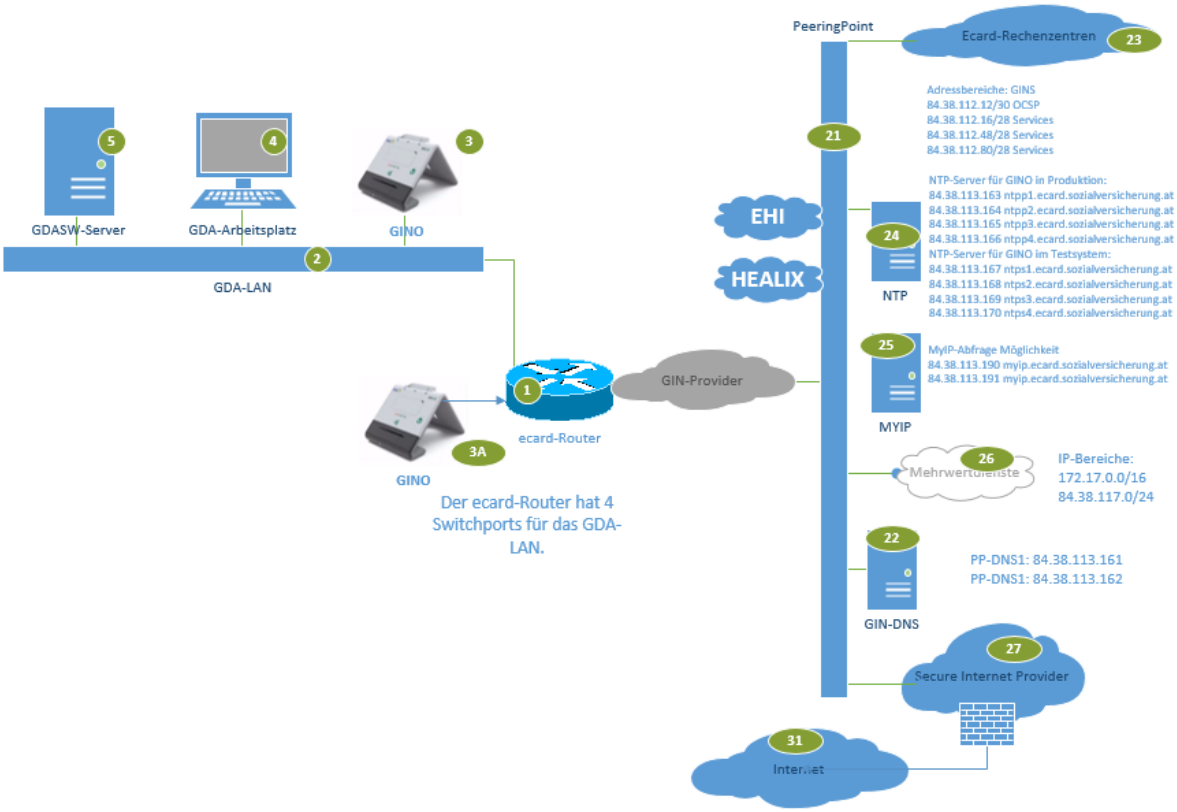

Abbildung 19: Minimalsetup eines VP-LANs mit e-card-Anschluss

- Der e-card Router hat vier GDA-LAN-Ports. In kleinen Ausprägungen sollen alle Kundengeräte direkt an den e-card Router angeschlossen werden. Symbolisch ist in der obigen Abbildung ein zweiter Kartenleser direkt am Router skizziert. Diese einfache Konstellation wird in diesem Dokument auch als „Referenz-System“ bezeichnet.

6.2 Prinzip der Realisierung – Routing

Ziel der Konfiguration ist es, für alle VPs eine Möglichkeit zu schaffen, das Routing mit vertretbarem Aufwand zu ermöglichen. Auch wenn dies nur in einer kleineren Zahl von VP-LANs tatsächlich notwendig ist, muss dennoch für einen „Bestandschutz“ vorhandener IT / Netzwerklösungen gesorgt werden.

Wichtige Prinzipien dieser Lösung:

- Die Routing Konfiguration ist konstant (GIN-Zugangsnetz Router) und wird nicht vor Ort durch den Provider individuell angepasst.
- Der GIN-Zugangsnetz Router empfängt RIPv2 (Routing Information Protokoll Version 2) Routing-Updates aus dem VP-LAN und lernt so die Routen „hinter“ dem privaten Router/Firewall.
- Der GIN-Zugangsnetz Router sendet niemals selbst Routing-Updates in das Netzwerk des VP!
  (Damit wird verhindert, dass es zu Konflikten im VP-LAN kommt, ein erhöhter Support-Aufwand verursacht und die Definition von Zuständigkeit bzw. Verantwortung für die Funktion der e-card Anwendung und der IT-Lösung sehr erschwert wird.)

Die folgende Darstellung zeigt ein mögliches Szenario.

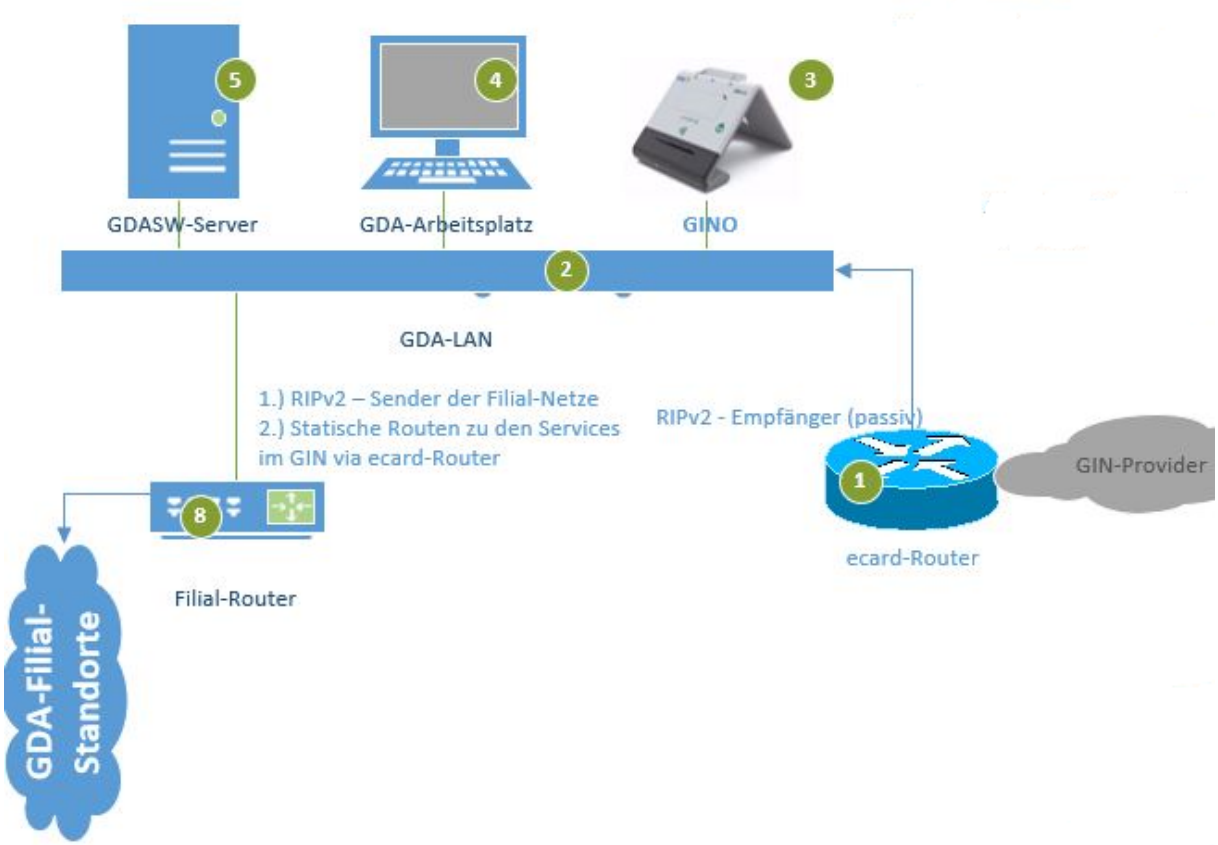

Abbildung 20: Routing im VP-LAN

Beschreibung:

(1) Die Schnittstelle „Zuständigkeit Provider“ ändert sich nicht, der Provider führt auch keine zusätzlichen Konfigurationen am Router aus.

(Außer DHCP – ON / OFF und bei Wunsch IP-Adresse des Routers)
Siehe auch Abschnitt: **2.3 Zuständigkeiten und Schnittstelle im VP-LAN**

(2) **WICHTIG:** der erste GINO ist am Router anzuschließen; damit wird auch (üblicherweise) die Abnahme durchgeführt.

(3) Der GIN-Router empfängt (nur lesend!) RIP2-Updates aus dem VP-LAN. **Er sendet aber niemals eigene RIP2-Updates aus.**

(4) Der lokale IT-DL kann nun seinerseits die notwendigen Routen per RIP2 propagieren (seine / die lokalen) und die Routen zum PP als statische Routen in „seinem“ Router konfigurieren. Gegebenenfalls (bei Internet-MWDs) konfiguriert er auch die Default Route zum VP-Router. Siehe auch Anmerkung „Statische Routen“ weiter unten.

(5) Das „Sub-Netzwerk des VP“ wird von der e-card Serviceline und von den Providern **nicht supportet** (z.B. auch Sub-LAN mittels VPN Verbindung!).

Um solche Konfigurationen **stabil und für alle Router konstant zu implementieren,** sind einige Parameter zu beachten bzw. zu konfigurieren, die im folgenden Abschnitt ausgeführt werden.

Statische Routen im „privaten“ Router/FW:

Die Routen, die vom IT-DL statisch in „seinem“ Router (6) zu konfigurieren sind, beinhalten mindestens folgende Routen:

- 84.38.112.0/20 (zentrale Services im RZ, PP und EHI, ELGA)
- 172.16.0.0 bis 172.31.255.255 (= 172.16.0.0/12) PP, MWD, Provider und RZ
- 79.174.96.0/19 (HEALIX)
- 193.46.140.0/24 (HEALIX)
- 193.46.141.0/24 (HEALIX)
- 193.46.142.0/24 (HEALIX)
- Um die Nutzung von Internet-MWDs über den PP zu ermöglichen, ist eine "Default-Route" zum GIN-Zugangsnetz Router erforderlich.

6.3 Technische Randbedingungen und Anforderungen

Die RIPv2-**Konfiguration ist konstant**, Netze aus **10.0.0.0/9** und **192.168.0.0/16** (oder Sub-Netze davon) werden unterstützt.
Wenn RIPv2 unterstützt werden soll, muss das verwendete VP-LAN ein Netz aus den freigegebenen Netzbereichen 10.0.0.0/9 oder 192.168.0.0/16 sein.

RIPv2 im GIN-Router ist als RIPv2-**Listener (reader-only)** ausgelegt!
Es werden **nur freigegebene Netze für das VP-LAN gelernt,** siehe weiter unten.
Der Routing-Table ist auf 200 Routen limitiert.
Die RIPv2-Konfiguration ist in jedem Router per Default vorhanden, kann aber bei der Herstellung des e-card Anschlusses auf Wunsch deaktiviert werden.

Freigegebene Netze für das VP-LAN (Arzt):
Netzbereich_1: 192.168.0.0 bis 192.168.255.255
Netzbereich_2 10.0.0.0 bis 10.127.255.255

Diese Netze oder Subnetze werden per RIP2 gelernt (wenn die IP-Adresse des Routers in Netzbereich_1 liegt) – **alle anderen nicht!**

6.4 Firewall (routing) (VP-LAN)

Eine z.B. größere Einrichtung / VP-LAN, die eine eigene 10.0.0.0 Netz-Adresse verwendet, kann das Netzwerk des VP als „Transfernetz“ zu seiner Infrastruktur verwenden.

Methode 1: Die lokale Firewall (6) (der Einrichtung oder des IT-DL) propagiert die Routing-Updates per RIPv2 auf das Transfersegment und trägt die statischen Routen zu den Services im GIN auf seiner Firewall ein (next-hop = e-card Router).

Methode 2: Anstatt Routing kann auch NAT verwendet werden. Jeder Host im VP-LAN kann auf eine IP im Transfer-LAN übersetzt werden. (Schlagwort: „Network-NAT“).
Es reicht aber auch ein „hide-NAT“ aus, da aus dem GIN keine Verbindungen aktiv in die Ordination aufgebaut werden. (Ausnahme: „FULL-NAT“ für spezielle MWD-Services)
Auch in diesem Fall sind die statischen Routen zu den Services im GIN auf seiner Firewall ein (next-hop = e-card Router) einzutragen.

In der folgenden Abbildung wird unter „3A“ der GINO gezeigt welcher der unterstützten Abnahmesituation durch den Provider-Techniker entspricht. Sowohl die Serviceline, als auch der Provider und SVC haben in dieser Konstellation die besten Möglichkeiten Fehler zu analysieren. Der GINO „3A“ hat in dem Fall eine IP-Adresse aus dem Transfer-LAN.

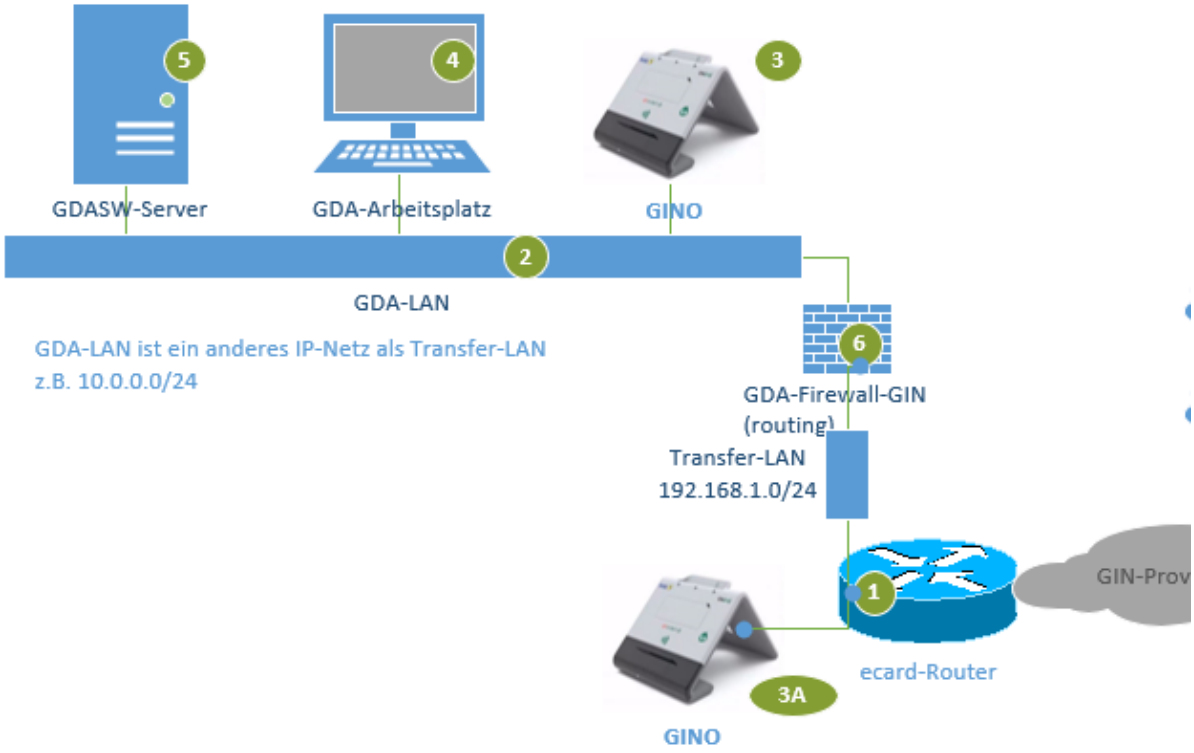

Abbildung 21: Schematische Darstellung VP-LAN

Wichtig:
Zumindest der erste GINO und mindestens ein Endgerät am Router sind eingerichtet → Abnahme der Installation erfolgt hier!
Ein denkbarer Ansatz in dieser Konstellation ist, bis zu drei GINOs direkt am Router zu betreiben (Router hat aktuell 4 Ports).

Wie in der Abbildung dargestellt, lassen sich „hinter“ dem eigenen Router auch mehrere Netze aus dem Bereich 10.0.0.0 bis 10.127.255.255 oder der 192.168er Netze verwenden, und so gegebenenfalls zusätzliche Anforderungen der Vernetzung der VP Standorte erfüllen.

Auf der privaten Firewall/Router müssen die Services wie in „VP-LAN – Kommunikation mit den Services im GIN (GINS)“ freigeschalten werden.

Der Support der e-card Serviceline endet aber immer vor der “privaten” Firewall/dem Router.

6.5 Routing mit lokalem Internetanschluss

Wie anhand der folgenden Skizzen ersichtlich ist, gibt es viele Konstellationen, die aktuell im Feld anzutreffen sind.
Diese führen aktuell zu Problemen, wenn VP-Systeme die zentralisierten Systeme im GINS erreichen wollen.

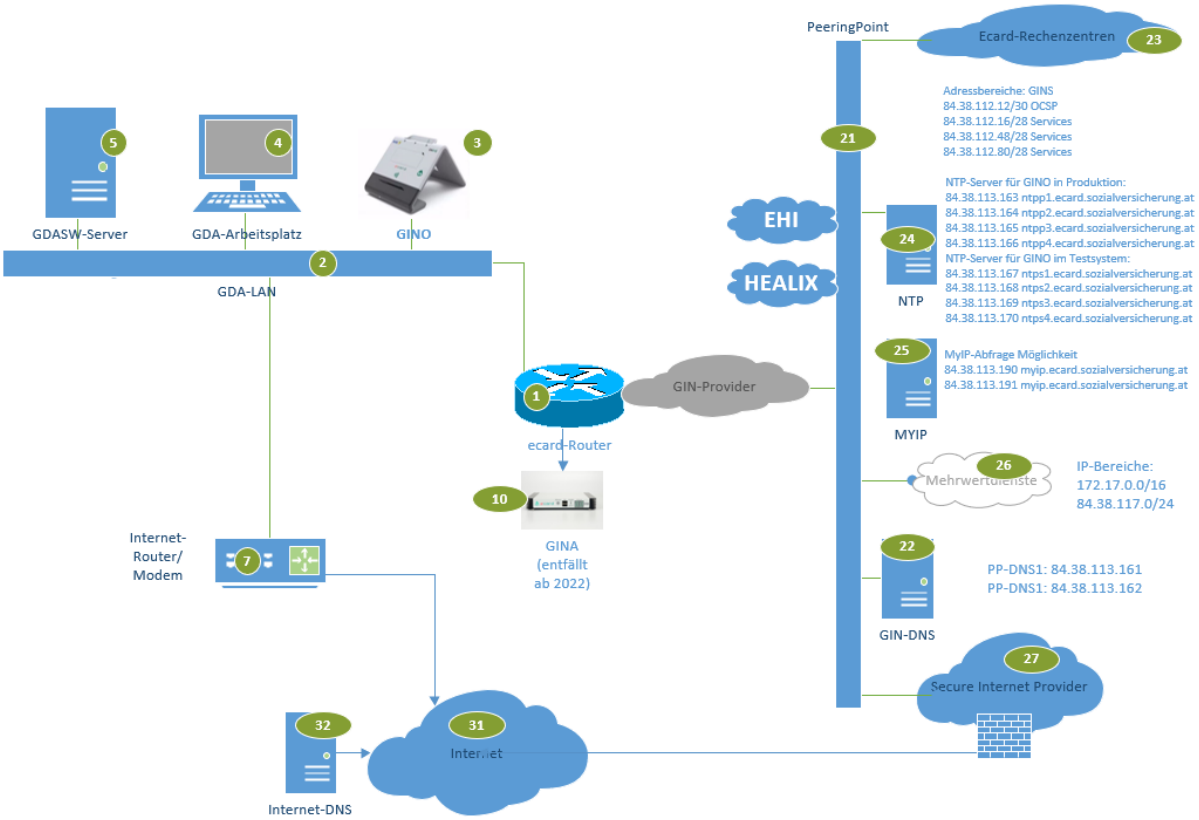

Abbildung 22: Skizze aktueller problematischer Konstellationen 1/2

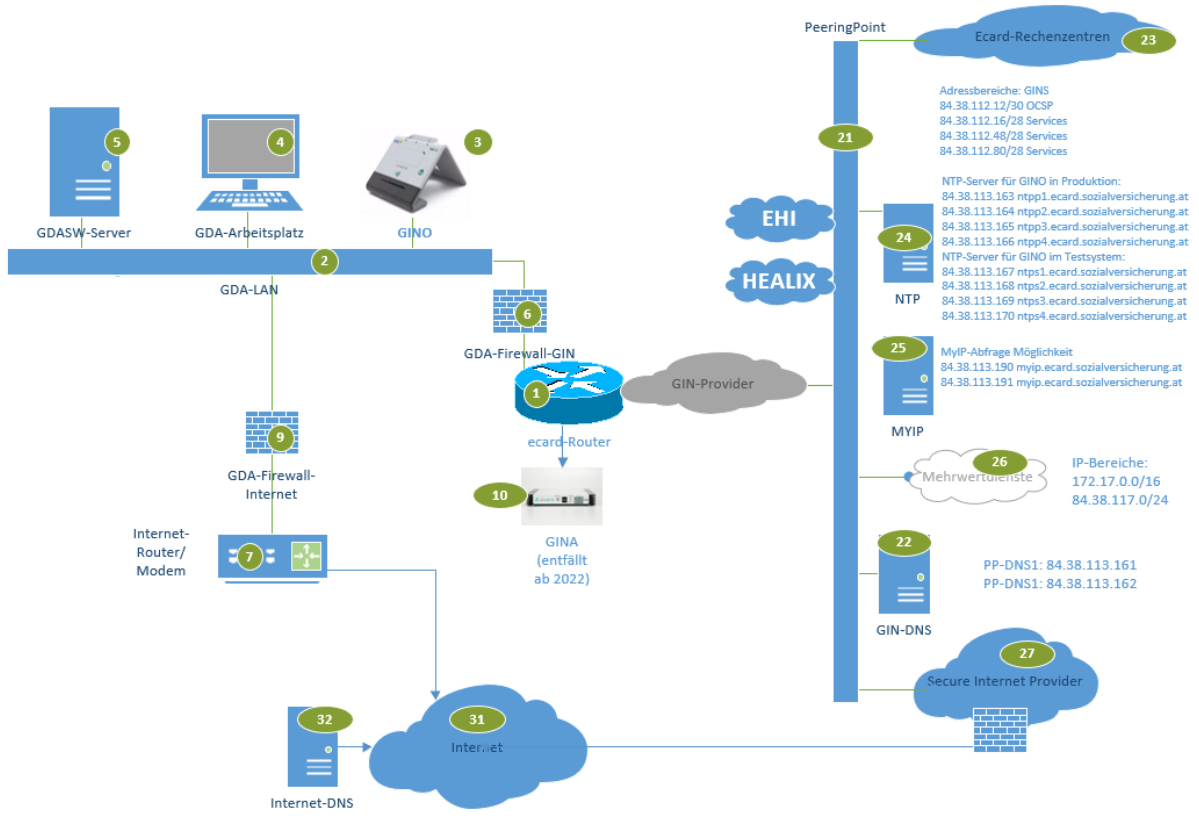

Abbildung 23: Skizze aktueller problematischer Konstellationen 2/2

„Gesamtübersicht eines Vollausbaues“ mit Filialen und lokalem Internet-Anschluss:

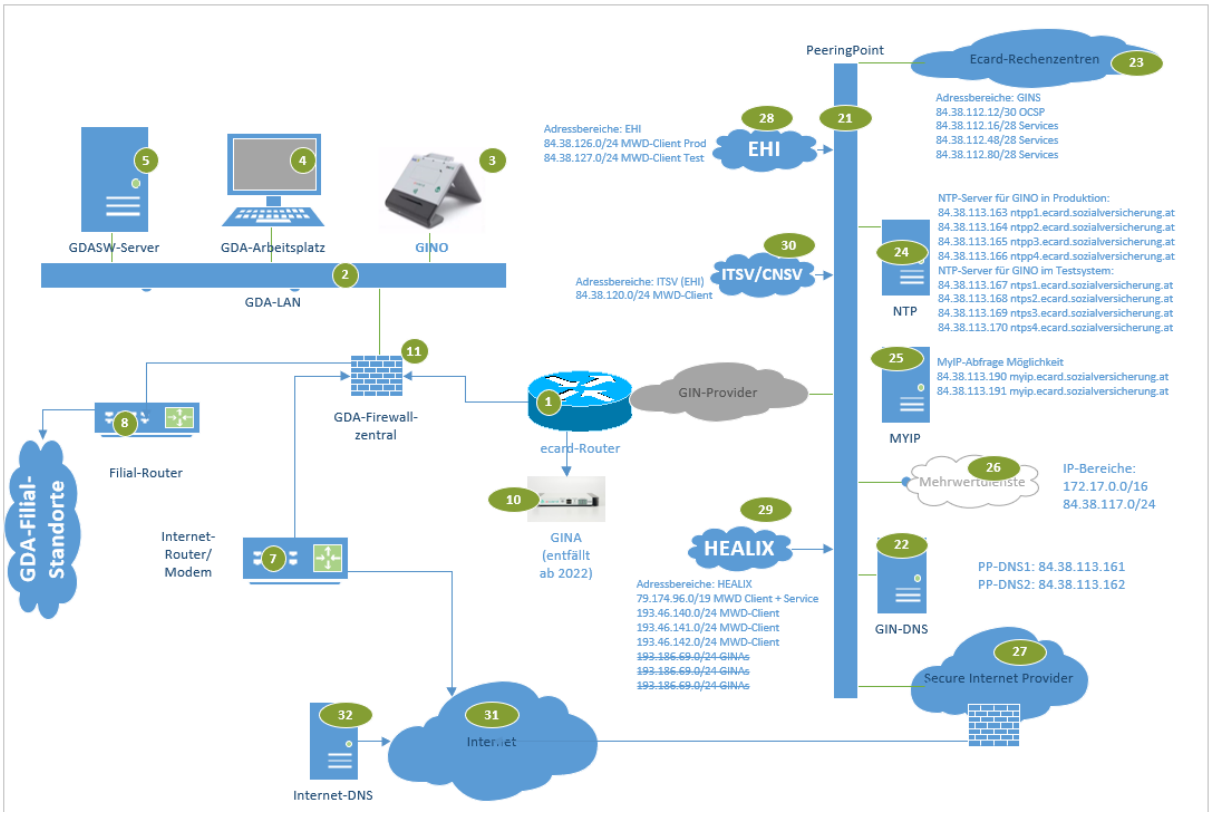

Abbildung 24: „Gesamtübersicht eines Vollausbaues“ mit Filialen und lokalem Internet-Anschluss

Problemstellung:

- Default-Gateway ins Internet
- Routen via e-card Router für Systeme die mit GINS kommunizieren
- DNS-Auflösung: Internet-DNS vs. PP-DNS

Lösungsansätze:

- Routen auf den VP-Systemen statisch eintragen
- Routen via DHCP-Optionen an die VP-Systeme verteilen
- Routen in die Internet-Router/Internet-FW eintragen
- GINO statisch konfigurieren – benötigt nur DNS und RZ-Kommunikation außerhalb des VPs → nie Internet!

Probleme:

- Dreieckskommunikation: mit stateful FWs bedarf es einer speziellen Konfiguration – nicht bei allen Herstellern lösbar
- Ausfall eines Gerätes führt zu Totalausfall
- Geräte (Internet-Router und FW), die vom Internet aus z.B. mit DDoS belastet werden, gefährden die Funktionen mit dem GINS – obwohl GINS vom Internet gänzlich isoliert ist

Dieser Abschnitt bietet Raum für Diskussionen – es gibt keine „ultimative beste Lösung“ für alle Ansprüche.
Ausführende Techniker sollten mit ihren Kunden geschäftskritische Applikationen identifizieren und das Design entsprechend danach ausrichten.

6.6 e-card „Referenz-System“ bei Routing und Firewalls

Da es sich bei den Konfigurationen mit zusätzlichen Routern und gegebenenfalls auch Firewalls in gewisser Weise um „Sonderlösungen“ handelt, bei denen der Support der Provider und der e-card Serviceline nicht vollständig greifen kann (für alles was „hinter“ einem Router oder einer Firewall installiert ist), wird dringend zu folgenden „Mindestmaßnahmen“ bzw. Vorkehrungen geraten:

- Ein Referenz-System (muss mindestens bei der Abnahme vorhanden sein, um den Support der e-card Serviceline und damit gegebenenfalls auch der Provider in Anspruch nehmen zu können: GINO am e-card Router angeschlossen, DHCP vom e-card Router oder statisch konfiguriert.)
- Das Referenz-System kann selbstverständlich auch ein „ganz normaler“ Arbeitsplatz sein, der im Störungsfall im VP-LAN immer funktionieren sollte.
- Dem SV-Partner ist dieser Zusammenhang mitzuteilen und gegebenenfalls auf die eigene Hotline des IT-DL oder VPSWH zu verweisen, wenn es zu Ausfällen VP-LAN bei solchen Installationen kommt.

Wichtige Hinweise:

Die e-card Serviceline ist in der Lage, die technische Funktion von Router und GINOs zu prüfen (wenn die GINOs ihre Health-informationen zur KALVE übertragen konnten und die Fernwartung aktiviert wurde).

Von allen anderen Komponenten, die sich hinter Routern oder Firewalls befinden, „weiß“ die e-card Serviceline nichts – und leistet auch keinen Support.

Einsätze von Providern, die durch solche Komponenten bzw. durch Fehler in diesen Komponenten ausgelöst werden, sind aus Sicht des Providers kostenpflichtig.

Die in diesem Abschnitt dargestellten Techniken geben den IT-DL vor Ort die Möglichkeit, flexibel auf die Wünsche ihrer Auftraggeber zu reagieren.

Wir bitten Sie daher, dem SV-Partner oder zuständigen Personen vor Ort die Zuständigkeiten im Netzwerk des VP für die einzelnen Komponenten klar darzulegen.

6.7 Praxisbeispiel „nicht freigegebene IP-Netze im GDA-LAN“ – Lösungsansatz mit NAT auf einer FW zwischen den GDA-LANs.

Rückfragen haben gezeigt, dass die Verwendung von „nicht freigegebenen IP-Bereichen“ in LANs des VP im Zuge der Umstellung auf GINS und der damit erforderlichen direkten Erreichbarkeit der Services im GIN zu den erwarteten Problemen führen.

Der Grund ist, dass die GIN-Provider dazu angehalten sind, keine IP-Pakete von Sourcen die nicht dem Adresskonzept entsprechen zu transportieren. Das ist dem Schutz des GIN und einem stabilen Betrieb geschuldet.

Das folgende Praxisbeispiel – welches aus einem realen Problem-Fall übernommen wurde – soll eine Idee liefern, wie diese Situation gelöst werden kann, ohne alle mit dem LAN verbundenen Geräte mit einem neuen IP-Bereich auszustatten. Das „Problem“ stellt eine IP-Adress-Überlappung mit im GIN existierenden Netzwerken dar – also im „nicht freigegebenen Adressbereich“ für VP-LANs. Langfristig ist eine IP-Anpassung der VP-LANs trotzdem sinnvoll.

Anmerkung zu überlappenden IP-Bereichen: Wenn lokal IP-Bereiche genutzt werden, die im GIN anderswo verwendet werden, kann dieser IP-Bereich im GIN trotz NAT nicht erreicht werden. → „Black Hole“-Situation

Als leicht nachvollziehbares Beispiel was mit „black hole“ gemeint ist – anhand des Internets und einem bekannten DNS-Services:
Wenn lokal das Netz 8.8.8.0/24 verwendet werden würde, dann kann der Google-DNS 8.8.8.8 im Internet nicht erreicht werden, da der lokale Rechner versucht 8.8.8.8 lokal im LAN zu finden (ARP). Natürlich gibt es seitens der Hersteller diverse „Tricks“, um auch solche Probleme zu meistern (z.B. „proxy-ARP“, „more specific route“ / „longest prefix“). Diese Lösungen sind nur unter bestimmten Voraussetzungen (8.8.8.8/32 lokal nicht in Verwendung) nutzbar und im Sinne eines langfristigen, problemlosen Betriebes nicht anzuraten. Sinngemäß verhält sich das in allen Netzwerken so – auch im GIN.

Lösungsansätze:

Es bieten sich zwei Varianten mit NAT auf der GDA-Firewall an.

6.7.1 1:1 NAT zwischen den beiden GDA-LANs

Eine Firewall (9) kann mittels NAT (1:1) die Rechner des „VP-LAN intern“ (2.2) in das VP-LAN (2) übersetzen und so eine Kommunikation mit dem GINS ermöglichen. Je nach Hersteller der Firewall kann das manuell oder mittels eines konfigurierbaren Automatismus (Network-NAT) erfolgen. In der Regel wird der Host-Anteil der IP-Adresse beibehalten. (Beispiel: VP-LAN intern (2.2) =10.239.0.**47**/24 entspricht im VP-LAN (2) =192.168.1.**47**/24.) Dies ermöglicht es die Zusammenhänge trotz NAT relativ einfach zu erkennen. Es bleibt grundsätzlich allen Rechnern des VPs möglich über die Firewall miteinander zu kommunizieren.

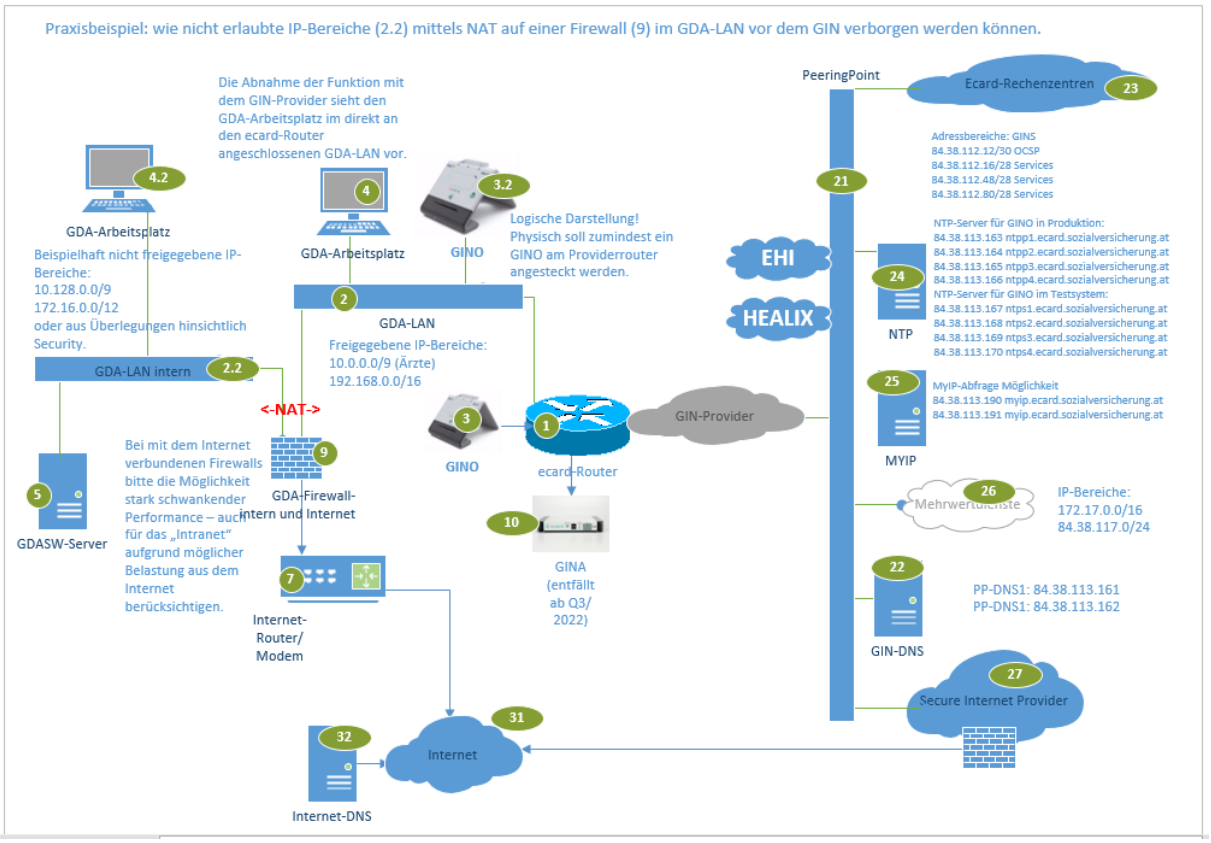

Abbildung 25: Skizze Praxisbeispiel 1:1-NAT

Aufmerksamkeit ist bei der Nutzung eines VP-internen DNS-Services für die Auflösung VP-interner Namen in Verbindung mit einer NAT-Konfiguration zwischen Client und DNS-Server geboten!

Beispiel:

- Client (4) versucht mittels DNS (5) die IP-Adresse des Rechners (4.2) aufzulösen.
- Der DNS-Server wird eine IP aus dem VP-LAN intern (2.2) als Antwort an den Client (4) schicken.
- Da dazwischen aber ein NAT ist, muss die Firewall auch die DNS-Antwort umschreiben – auf die NAT-IP entsprechend dem VP-LAN (2). Viele Firewalls machen das automatisch (Schlagwort: DNS-rewrite).

6.7.2 Hide-NAT (Overload-NAT) zwischen beiden VP-LANs

Eine Firewall (9) kann mittels Hide-NAT (many:1) die Rechner des „VP-LAN intern" (2.2) in das VP-LAN (2) auf eine IP-Adressen übersetzen und so eine Kommunikation mit dem GINS ermöglichen. Nachteil dieser Lösung ist, dass der Rechner (4 – siehe Skizze 1:1 NAT zwischen den beiden VP-LANs) im VP-LAN nicht mehr ohne weitere NAT-Regeln in das VP-LAN-intern (2.2) zugreifen kann.
Wenn kein Rechner im VP-LAN (2) betrieben wird, sondern nur GINOs, ist das eine einfache Möglichkeit. Zu bedenken ist jedoch, dass im „Ent-Störungsfall" ein Rechner

– wenn auch temporär – direkt im, an den e-card Router (1) angeschlossen VP-LAN (2) betrieben werden muss (z.B. direkt auf einem Port des Routers).

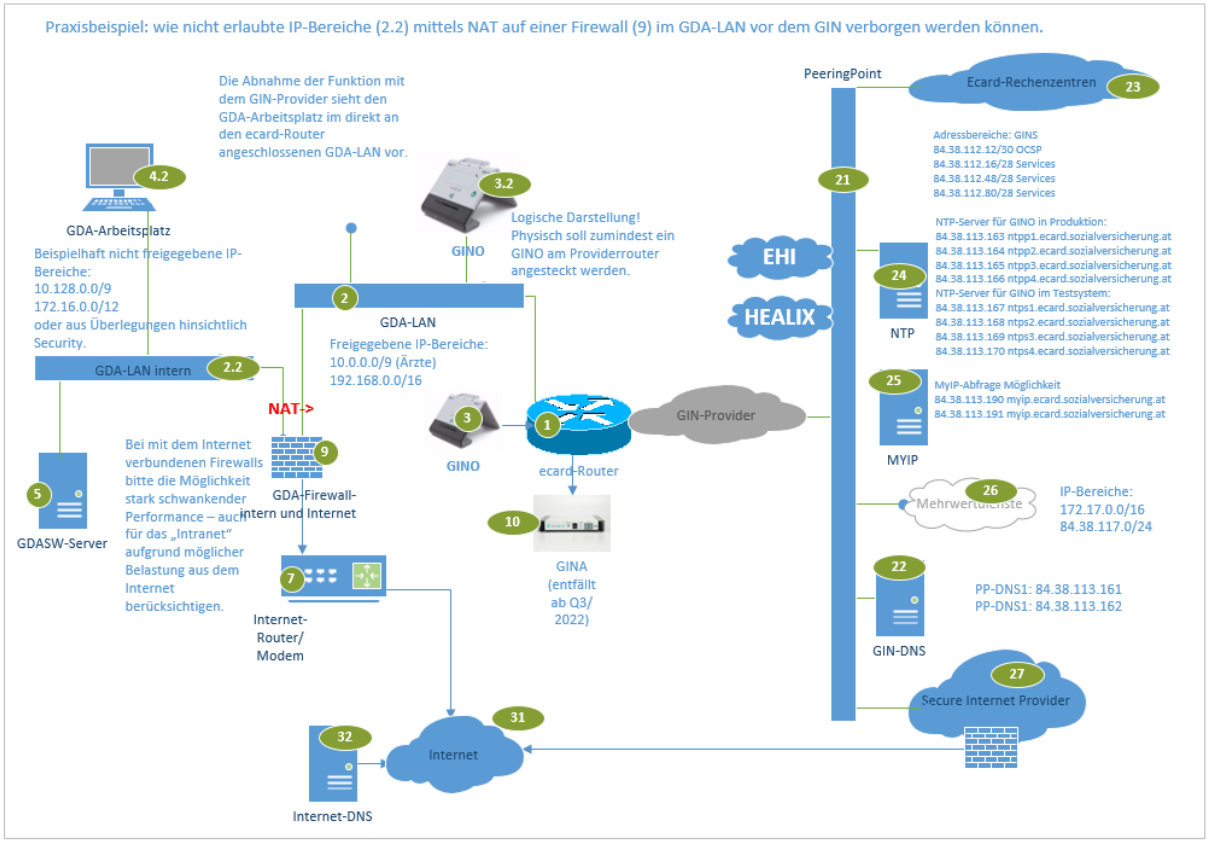

Abbildung 26: Skizze Praxisbeispiel Hide-NAT

6.7.3 Routing auf der Firewall (für beide Varianten)

Statische Routen zu den Zielen im GIN müssen über den Next-Hop e-card Router (1) auf der Firewall eingetragen werden. Siehe Punkt **6.2 Prinzip der Realisierung – Routing**.

Das RIPv2-Routing ist in diesem Fall nicht erforderlich. Der e-card Router (1) benötigt keine Information über das hinter dem NAT verborgene Netzwerk (2.2).

6.7.4 Generelle Anmerkungen zu diesem Praxisbeispiel

Wir empfehlen ausdrücklich keine komplizierten Lösungen zu bauen, wenn es keinen guten Grund dafür gibt. Trotz des Umstands, dass diverse Techniken, wie hier beschrieben, durchaus machbar und längst etabliert sind, sollte eine simple und stabile Lösung angestrebt werden.
Das nachträgliche Ändern von IP-Bereichen ist unter Umständen einmalig aufwändig, kann sich aber im Vergleich mit der Komplexität in Firewalls trotzdem schnell rechnen.
Dieses Beispiel stellt also keine Aufforderung dar, grundsätzlich eine Firewall mit NAT zwischen den e-card Router und dem VP-LAN zu etablieren.

7 Firewall transparent (VP-LAN)

Eine zusätzliche Firewall im VP-LAN zur „Absicherung“ der e-card Services ist aus Sicherheitsaspekten heraus nicht erforderlich. Siehe auch Abschnitt: **2.6 Sicherheitsaspekte (informell)**

Nachfolgend eine Abbildung einer solchen Konfiguration, unter Annahme einer transparent eingebauten Firewall:

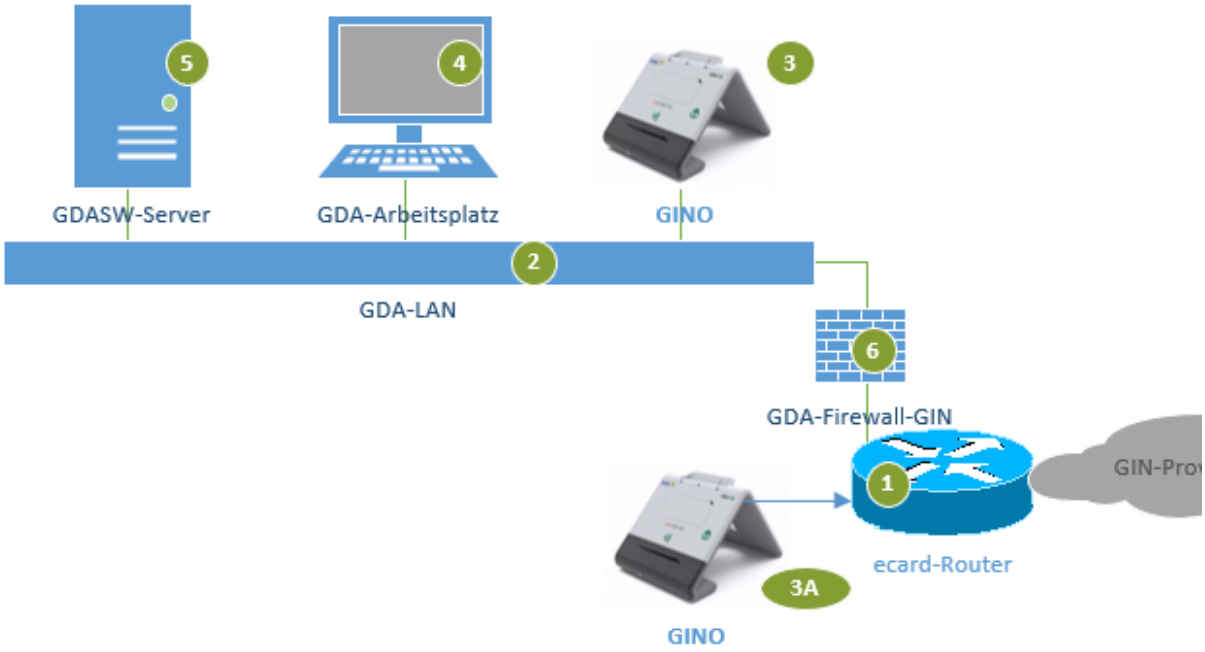

Abbildung 27: Firewall - Prinzip Ansicht - GINA

(1) Wird eine transparente Firewall (6) zwischen GIN-Zugangsnetz Router (1) und dem VP-LAN (2) eingesetzt, so ist mindestens ein „Test-Referenz-System“ vorzubereiten und für technische „Notfälle“ zur Verfügung zu haben. Eine Abnahme durch den Provider erfolgt nur an diesem System. Auch der Support der e-card Serviceline erstreckt sich nur auf direkt angeschlossene GINOs (3A).

(2) Alle Einrichtungen (Betrieb, Konfiguration, Störungsbeseitigung, etc.), die sich hinter einer Firewall befinden, sind durch den IT-Dienstleister vor Ort zu pflegen / zu warten. **Dies ist dem SV-Partner eindeutig mitzuteilen. Treten Serviceeinsätze für die Provider auf, deren technische Ursache hinter der Firewall liegt, so werden diese vom Provider kostenpflichtig verrechnet. Zu einer Störungsbeseitigung ist er nicht verpflichtet.**

(3) Die Kommunikation zwischen den Endgeräten in (3, 4, 5) – sprich GINO, PCs und Server mit dem GINS ist durch den IT-DL oder VPSWH zu gewährleisten (Firewall-Konfiguration).

(4) Die zentralen Services müssen für die unten aufgeführten Ports aus dem VP-LAN erreichbar sein.

7.1 VP-LAN – Kommunikation mit den Services im GIN (GINS)

Anmerkungen und Konfigurationsinfos:

Im Folgenden sind die (aktuell) verwendeten IP-Ports aufgelistet. Diese können sich in der weiteren Entwicklung des Systems und gegebenenfalls weiterer Applikationen entsprechend ändern.

Bezeichnung	Port	Direction	Bemerkung
domain	UDP 53	VP-PC → PP-DNS	DNS
domain	UDP 53	GINO → PP-DNS	DNS
www	TCP 80	VP-PC → Zentrale Services	myip.ecard.sozialversicherung.at, ocsp.ecard.sozialversicherung.at, noch CCS
https	TCP 443	VP-PC → Zentrale Services	verschlüsselte Kommunikation zur mit SS12/Applikation und Webbrowser
http/https	TCP 80/443	VP-PC → GINO	
kalve-fw/http	TCP 451	GINO → Zentrale Services	KALVE
kalve-download/http	TCP 452	GINO → Zentrale Services	KALVE
kalve-noauth/https	TCP 453	GINO → Zentrale Services	KALVE
kalve-auth/https	TCP 454	GINO → Zentrale Services	KALVE
ssh	TCP 10022, 20022	GINO-> Zentrale Services	Fernwartung via KALVE. Nur wenn der GINO über diese Ports eine Verbindung aufbauen kann, kann er ferngewartet werden.
ntp	UDP 123	GINO → Zentrale Services	Gesichertes NTP
Alle Systeme	Mindestens ICMP Type 0,8,11	Alle Systeme → alle Systeme/IP-Adressen	Fehlersuche, Analyse

Alle Systeme	Mindestens UDP 33434-33529	Alle Systeme → alle Systeme/IP-Adressen	Fehlersuche, Analyse

Abbildung/Tabelle 28: Port – GDA → Zentrale Services

7.2 VP-LAN – Kommunikation mit MWD-Services

Vergleichbar mit den Services für e-card und ELGA, bedarf es bei einer Firewall zwischen e-card Router und VP-LAN der „Freischaltung“ der gebuchten MWD-Services.

8 Informationssammlung: „Fakten auf einem Blatt“

Dieser Abschnitt soll alle Namen, IPs, Routen für Techniker zusammenfassen.

8.1 Übergreifende Systeme

8.1.1 PP-DNS:

- PP-DNS1 (vormals EHI-MWD-DNS1) 84.38.113.161
- PP-DNS2 (vormals EHI-MWD-DNS2) 84.38.113.162

8.1.1.1 Für GINS (e-card/ELGA) relevante DNS-Zonen

- ecard.sozialversicherung.at
- ecard-test.sozialversicherung.at
- pki.sozialversicherung.at

8.1.2 Routen/Netze ins/im GIN:

- 10.0.0.0/9 für die Verwendung im VP-LAN freigegeben
- 10.128.0.0/9 für die Verwendung im GIN zur VP-Adressierung (Provider-Link, NAT-IPs)
- 79.174.96.0/19 (HEALIX)
- 84.38.112.0/20 (zentrale Services im RZ, PP und EHI, ELGA)
- 172.16.0.0 bis 172.31.255.255 (= 172.16.0.0/12) PP, MWD, GIN-Provider und RZ
- 192.168.0.0/16 für die Verwendung im VP-LAN freigegeben
- 193.46.140.0/24 (HEALIX)
- 193.46.141.0/24 (HEALIX)
- 193.46.142.0/24 (HEALIX)
- 193.186.69.0/24 (HEALIX)
- 193.186.69.0/24 (HEALIX)
- 193.186.69.0/24 (HEALIX)
- 0.0.0.0/0 Defaultroute ins GIN (empfohlen; notwendig für Secure-Internet)

8.1.3 QoS

Im GIN ist ein dreistufiges QoS-Konzept implementiert das von allen Providern umgesetzt ist. Der GDA-SWH oder Benutzer muss hierzu nichts berücksichtigen, die Konfiguration gewährleistet eine möglichst gute Verbindung zu den zentralen Services.
Die Detailkonfiguration für die Provider findet sich im Providerdokument.

8.1.4 OCSP

OCSP Server werden von PC, KIS System, Arztsoftware benötigt, um die Vertrauenswürdigkeit der zentralen Services (GINS) z.B. von https://services.ecard.sozialversicherung.at zu überprüfen (ob die e-card Root/Serverzertifikate gültig sind). Auch wenn der PC den GINO anspricht, kann der PC die Serverzertifikate des GINOs auf Gültigkeit prüfen. Der GINO prüft auch die Gültigkeit der Serverzertifikate der Kartenleser-Verwaltung (KALVE).
Stellen Sie bitte unbedingt die Erreichbarkeit dieser Services sicher!

8.2 VPSWH-Umgebung

Die folgenden IP-Adressen sind zum besseren Verständnis zusätzlich angegeben. Der direkte Aufruf der Services über die IP-Adressen ist nicht unterstützt.

8.2.1 OCSP Service für Test-Referenzsysteme

ocsp-test.pki.sozialversicherung.at via PP-DNS: 84.38.112.12
ocsp-test.pki.sozialversicherung.at via Internet-DNS: 84.38.112.13
ocsp.ecard.sozialversicherung.at via PP-DNS: 84.38.114.120
ocsp.ecard.sozialversicherung.at via Internet-DNS: 212.183.22.90

8.2.2 ECARD/ELGA/TRANSFER-Services

services-a.ecard-test.sozialversicherung.at via PP-DNS: 84.38.112.28
services-a.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.112.29
kalve-a.ecard-test.sozialversicherung.at via PP-DNS: 84.38.112.28
kalve-a.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.112.29
ssh-a-a.ecard-test.sozialversicherung.at via PP-DNS: 84.38.112.28
ssh-b-a.ecard-test.sozialversicherung.at via PP-DNS: 84.38.112.28
ssh-a-a.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.112.29
ssh-b-a.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.112.29
elga-a.ecard-test.sozialversicherung.at via PP-DNS: 84.38.112.58
elga-a.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.112.59
transfer-a.ecard-test.sozialversicherung.at via PP-DNS: 84.38.112.88
transfer-a.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.112.89

8.2.3 MyIP-Auskunftsservice

myip.ecard-test.sozialversicherung.at via PP-DNS: 84.38.113.190
myip.ecard-test.sozialversicherung.at via Internet-DNS: 84.38.113.191

8.2.4 NTP (gesichert) für GINOs

ntps1.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.167
ntps2.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.168
ntps3.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.169
ntps4.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.170

8.2.5 Freischaltungen VPSWH/Referenz-System

Erforderliche Freischaltungen **übergreifend** für VPSWH **und** PROD						
Client-System (Source)	Destination DNS-Name	Destination IP-Adresse	IP-Protokoll	Port-nummer	Verwendung	Anmerkung
DNS-Server (KA intern) bzw. Client-Systeme, GINO	ehi-mwd-ns1.ecard.ginet.at	84.38.113.161	UDP	53	DNS-Auflösung/Forward	
	ehi-mwd-ns2.ecard.ginet.at	84.38.113.162	UDP	53	DNS-Auflösung/Forward	
KIS/VPSW, PC mit Browser, GINO	myip.ecard.sozialversicherung.at	84.38.113.190 + 84.38.113.191	TCP	80	Selfservice Client-IP	
KIS/VPSW, PC mit Browser, GINO	ocsp.ecard.sozialversicherung.at	84.38.114.120	TCP	80	OCSP via http	Server-Zertifikate der Services
KIS/VPSW, PC mit Browser	GINOs	interne/private IP des GINOs	TCP	80 + 443	Client Zugriff auf GINO	Innerhalb der GDA-Infrastruktur
Alle Systeme	alle Systeme/IP-Adressen	alle in dieser Aufstellung	ICMP	Type 0, 8, 11	Fehlersuche, Analyse	Ping, Traceroute
Alle Systeme	alle Systeme/IP-Adressen	alle in dieser Aufstellung	UDP	33434 - 33529	Fehlersuche, Analyse	Traceroute mit UDP

Erforderliche Freischaltungen **explizit** für VPSWH						
Client-Test-System (Source)	Destination DNS-Name	Destination IP-Adresse	IP-Protokoll	Port-nummer	Verwendung	Anmerkung
KIS/VPSW, PC mit Browser, GINO	ocsp-test.pki.sozialversicherung.at	84.38.112.12 + 84.38.112.13	TCP	80	OSCP via http	KALVE/GINO-Zertifikate
KIS/VPSW, PC mit Browser	services-a.ecard-test.sozialversicherung.at	84.38.112.28 + 84.38.112.29	TCP	80 + 443	e-card Services	
GINO	kalve-a.ecard-test.sozialversicherung.at		TCP	451, 452	KALVE http	
			TCP	453, 454	KALVE https	
GINO	ssh-a-a.ecard-test.sozialversicherung.at		TCP	10022 + 20022	Fernwartung	
GINO	ssh-b-a.ecard-test.sozialversicherung.at		TCP	10022 + 20022	Fernwartung	
KIS/VPSW, PC mit Browser	elga-a.ecard-test.sozialversicherung.at	84.38.112.58 + 84.38.112.59	TCP	80 + 443	elga Services	
KIS/VPSW, PC mit Browser	transfer-a.ecard-test.sozialversicherung.at	84.38.112.88 + 84.38.112.89	TCP	80 + 443	File up/down-load	
GINO	ntps1.ecard.sozialversicherung.at	84.38.113.167	UDP	123	Zeitsynchronisation GINO	
	ntps2.ecard.sozialversicherung.at	84.38.113.168	UDP	123	Zeitsynchronisation GINO	
	ntps3.ecard.sozialversicherung.at	84.38.113.169	UDP	123	Zeitsynchronisation GINO	
	ntps4.ecard.sozialversicherung.at	84.38.113.170	UDP	123	Zeitsynchronisation GINO	

8.3 Produktions-Umgebung (Vertragspartner)

Die folgenden IP-Adressen sind zum besseren Verständnis zusätzlich angegeben.
Der direkte Aufruf der Services über die IP-Adressen ist nicht unterstützt.

8.3.1 OCSP Service

ocsp.pki.sozialversicherung.at via PP-DNS: 84.38.112.14
ocsp.pki.sozialversicherung.at via Internet-DNS: 84.38.112.15
ocsp.ecard.sozialversicherung.at via PP-DNS: 84.38.114.120
ocsp.ecard.sozialversicherung.at via Internet-DNS: 212.183.22.90

8.3.2 ECARD/ELGA/TRANSFER-Services

services.ecard.sozialversicherung.at via PP-DNS: 84.38.112.30
services.ecard.sozialversicherung.at via Internet-DNS: 84.38.112.31
kalve.ecard.sozialversicherung.at via PP-DNS: 84.38.112.30
kalve.ecard.sozialversicherung.at via Internet-DNS: 84.38.112.31
ssh-a.ecard.sozialversicherung.at via PP-DNS: 84.38.112.30
ssh-b.ecard.sozialversicherung.at via PP-DNS: 84.38.112.30
ssh-a.ecard.sozialversicherung.at via Internet-DNS: 84.38.112.31
ssh-b.ecard.sozialversicherung.at via Internet-DNS: 84.38.112.31
elga.ecard.sozialversicherung.at via PP-DNS: 84.38.112.60
elga.ecard.sozialversicherung.at via Internet-DNS: 84.38.112.61
transfer.ecard.sozialversicherung.at via PP-DNS: 84.38.112.90
transfer.ecard.sozialversicherung.at via Internet-DNS: 84.38.112.91

8.3.3 MyIP-Auskunftsservice

myip.ecard.sozialversicherung.at via PP-DNS: 84.38.113.190
myip.ecard.sozialversicherung.at via Internet-DNS: 84.38.113.191

8.3.4 NTP (gesichert) für GINOs

ntpp1.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.163
ntpp2.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.164
ntpp3.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.165
ntpp4.ecard.sozialversicherung.at via PP+Internet-DNS: 84.38.113.166

8.3.5 Freischaltungen Produktiv-System

Erforderliche Freischaltungen **übergreifend** für VPSWH **und** PROD						
Client-System (Source)	Destination DNS-Name	Destination IP-Adresse	IP-Protokoll	Port-nummer	Verwendung	Anmerkung
DNS-Server (GDA intern) bzw. Client-Systeme, GINO	ehi-mwd-ns1.ecard.ginet.at	84.38.113.161	UDP	53	DNS-Auflösung/ Forward	
	ehi-mwd-ns2.ecard.ginet.at	84.38.113.162	UDP	53	DNS-Auflösung/ Forward	
KIS/VPSW, PC mit Browser, GINO	myip.ecard.sozialversicherung.at	84.38.113.190 + 84.38.113.191	TCP	80	Selfservice Client-IP	
KIS/VPSW, PC mit Browser, GINO	ocsp.ecard.sozialversicherung.at	84.38.114.120	TCP	80	OCSP via http	Server-Zertifikate der Services
KIS/VPSW, PC mit Browser	GINOs	interne/private IP des GINOs	TCP	80 + 443	Client Zugriff auf GINO	
Alle Systeme	alle Systeme/IP-Adressen	alle in dieser Aufstellung	ICMP	Type 0, 8, 11	Fehlersuche, Analyse	Ping, Traceroute
Alle Systeme	alle Systeme/IP-Adressen	alle in dieser Aufstellung	UDP	33434-33529	Fehlersuche, Analyse	Traceroute mit UDP

Erforderliche Freischaltungen **explizit** für PROD						
Client-Prod-System (Source)	Destination DNS-Name	Destination IP-Adresse	IP-Protokoll	Port-nummer	Verwendung	Anmerkung
KIS/VPSW, PC mit Browser, GINO	ocsp.pki.sozialversicherung.at	84.38.112.14 + 84.38.112.15	TCP	80	OSCP via http	KALVE/ GINO-Zertifikate
KIS/VPSW, PC mit Browser	services.ecard.sozialversicherung.at	84.38.112.30 + 84.38.112.31	TCP	80 + 443	e-card Services	
GINO	kalve.ecard.sozialversicherung.at		TCP	451, 452	KALVE http	
			TCP	453, 454	KALVE https	
GINO	ssh-a.ecard.sozialversicherung.at		TCP	10022 + 20022	Fernwartung	
GINO	ssh-b.ecard.sozialversicherung.at		TCP	10022 + 20022	Fernwartung	
KIS/VPSW, PC mit Browser	elga.ecard.sozialversicherung.at	84.38.112.60 + 84.38.112.61	TCP	80 + 443	elga Services	
KIS/VPSW, PC mit Browser	transfer.ecard.sozialversicherung.at	84.38.112.90 + 84.38.112.91	TCP	80 + 443	File up/down-load	
GINO	ntpp1.ecard.sozialversicherung.at	84.38.113.163	UDP	123	Zeitsynchronisation GINO	
	ntpp2.ecard.sozialversicherung.at	84.38.113.164	UDP	123	Zeitsynchronisation GINO	
	ntpp3.ecard.sozialversicherung.at	84.38.113.165	UDP	123	Zeitsynchronisation GINO	
	ntpp4.ecard.sozialversicherung.at	84.38.113.166	UDP	123	Zeitsynchronisation GINO	

9 Abbildungsverzeichnis

Abbildung 1: Schematische Darstellung vom GDA-LAN zum Rechenzentrum 6
Abbildung 2: Struktur des GIN 7
Abbildung 3: Schnittstelle im VP-LAN 9
Abbildung 4: Maske aus der e-card Web-Oberfläche 10
Abbildung 5: Kommunikation im GIN 11
Abbildung 6: Wichtige IP-Adressen im VP-LAN 15
Abbildung 7: GINO User Interface – „Login“ Maske 24
Abbildung 8: GINO User Interface – Geräteinformation 24
Abbildung 9: GINO User Interface – Allgemein 25
Abbildung 10: GINO User Interface – Passwort Änderung 25
Abbildung 11: GINO User Interface – Netzwerk 26
Abbildung 12: GINO User Interface – Netzwerk (NTP Einstellungen) 26
Abbildung 13: GINO User Interface – Konfiguration & Firmware 1/2 27
Abbildung 14: GINO User Interface – Konfiguration & Firmware 2/2 27
Abbildung 15: GINO User Interface – Diagnose & Reporting 28
Abbildung 16: Namensauflösung für Mehrwertdienste 31
Abbildung 17: lokales DNS im Netzwerk des VP 32
Abbildung 18: Ordination mit LAN und PCs 34
Abbildung 19: Minimalsetup eines VP-LANs mit e-card-Anschluss 37
Abbildung 20: Routing im VP-LAN 38
Abbildung 21: Schematische Darstellung VP-LAN 41
Abbildung 22: Skizze aktueller problematischer Konstellationen 1/2 42
Abbildung 23: Skizze aktueller problematischer Konstellationen 2/2 42
Abbildung 24: „Gesamtübersicht eines Vollausbaues“ mit Filialen und lokalem Internet-Anschluss 43
Abbildung 25: Skizze Praxisbeispiel 1:1-NAT 46
Abbildung 26: Skizze Praxisbeispiel Hide-NAT 47
Abbildung 27: Firewall - Prinzip Ansicht - GINA 48
Abbildung/Tabelle 28: Port – GDA → Zentrale Services 50

9.1 Abkürzungen

ASWH	Arzt-Softwarehersteller
eSV	„e-Sozialversicherung“ – Internetportal der Sozialversicherungen
e-card Router	GIN-Router
GIN	Gesundheits-Informations-Netz
GDA	Gesundheitsdienste Anbieter (Ärzte, Apotheker, …)
GINA	Gesundheits-Informations-Netz-Adapter (läuft ab 2022 aus)
GINO	Nachfolger des LAN-CCR mit zusätzlichen Funktionen
GINS	Gesundheits-Informations-Netz-Services
IT-DL	IT-Dienstleister
KALVE	Karten Leser Verwaltung
LAN-CCR	LAN-Chip-Card-Reader oder auch LAN-Card Reader oder auch Kartenleser – LAN (läuft ab 2022 aus)
MWD-VPN	Mehrwertdienste-VPN
PP	Peering Point
PPG	Peering Point Betriebsgesellschaft mbH
SV-VPN	Sozialversicherungs-VPN
VPN	Virtual Private Network
VP	Vertragspartner
VPSWH	Vertragspartner Softwarehersteller