

## Kurzanleitung zum Connectivity Check Service CCS Version 1.6 (Stand: Mai 2022)

In diesem Dokument finden sich Informationen zur Architekturumstellung des e-card Systems und zum Connectivity Check Service, mit welchem geprüft werden kann, ob eine aktuelle Netzwerkinstallation den Anforderungen entspricht, die nach dem Abbau der GINA und dem Tausch von LAN-CCR gegen GINO erforderlich sind.

Dieses Dokument wird laufend um neue Inhalte erweitert. Änderungen/Neuerungen sind farblich markiert. Dabei wird bei einem komplett neu eingefügten Kapitel nur die Überschrift hinterlegt.

### Änderungshistorie

Datum	Inhalt	Version
26.05.2021	Initialversion	1.0
13.08.2021	Kapitel „5 Allgemeine Hinweise zum VP-Netzwerk“ hinzugefügt; weitere kleinere Ergänzungen	1.1
13.09.2021	Kapitel „4.2 Manuelle Testmöglichkeiten“ hinzugefügt, kleiner Ergänzungen	1.2
23.11.2021	Kapitel 1.1. Vorgehensweise für IT-Betreuer hinzugefügt Kapitel 4.1.3 und 4.1.4 hinzugefügt	1.3
9.12.2021	Aktualisierungen bezüglich OCSP	1.4
01.03.2022	Kapitel 5.1 DNS Server-Umgang, Kapitel 5.1.1 DNS Weiterleitung für pki.sozialversicherung.at ergänzt Kapitel 5.2 Hinweis „Änderungen oder Eintragungen von Routen am e-card GIN-Router sind nicht erforderlich“ Kapitel 5.2.2 Angleichung Apothekennetze an andere VP-Netze → Umstellung bis 31.05.2027 Kapitel 5.2.3 DNS Hinweis → wegen inhaltlicher Äquivalenz zu Kapitel 5.1 entfernt und mit entspr. Verweis versehen Kapitel 5.2.4 Entfernung der Healix-GINA Routen Kapitel 5.2.9 GINA-IP vs. Client-IP / Anschluss-IP – MyIP Auskunftsservice hinzugefügt Wording angepasst	1.5
09.05.2022	Kapitel 5.1 DNS Forward Korrektur Kapitel 5.2.2 Hinweis zum „Full NAT“ IP-Bereich hinzugefügt Kapitel 5.3 Nating von LAN-CCRs und CCS hinzugefügt	1.6

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitende Informationen .....</b>	<b>3</b>
1.1	Vorgehensweise für IT-Betreuer .....	3
1.2	Unterlagen und weitere Dokumentationen.....	3
<b>2</b>	<b>Allgemeine Informationen .....</b>	<b>5</b>
2.1	Big Picture / Motivation .....	5
2.1.1	Software-Umstellung .....	5
2.1.2	Hardware-/Netzwerkumstellung.....	6
<b>3</b>	<b>Kurzanleitung zur CCS Implementierung .....</b>	<b>9</b>
3.1	Erreichbarkeit des GINS prüfen .....	9
3.1.1	Überblick Vorgehensweise .....	9
3.1.2	Vorgehensweise Details.....	9
3.2	Ergebnisabfrage des Kartenleser-„Selbsttests“ .....	13
<b>4</b>	<b>Fehlerbehandlung/Ergebnisauswertung.....</b>	<b>14</b>
4.1	Mögliche Ursachen bei fehlschlagenden Tests .....	14
4.1.1	Aufruf der /check oder /checkDetails Ressource schlägt fehl.....	14
4.1.2	Aufruf von /checkDetails liefert keine Information zum Kartenleser .....	15
4.1.3	Fehlermeldungen bei Nutzung der Web-Oberfläche und mögliche Behebung .....	15
4.1.4	Weitere mögliche Fehlerursachen .....	16
4.2	Manuelle Testmöglichkeiten .....	17
4.2.1	DNS-Auflösung .....	17
4.2.2	Erreichbarkeit des GINS .....	18
4.2.3	Direkte Erreichbarkeit des LAN-CCR.....	19
4.2.4	Erreichbarkeit des GINS durch den LAN-CCR .....	20
<b>5</b>	<b>Allgemeine Hinweise zum VP-Netzwerk.....</b>	<b>21</b>
<b>5.1</b>	<b>DNS Auflösung.....</b>	<b>21</b>
5.1.1	Verwendung eines internen DNS im VP-Netzwerk.....	21
5.1.2	Verwendung eines öffentlichen DNS .....	21
5.2	DNS und Routing im VP-Netzwerk – Zusammenfassung .....	22
5.2.1	Ausgangslage .....	22
<b>5.2.2</b>	<b>Interne VP-Netze.....</b>	<b>22</b>
5.2.3	DNS Hinweise .....	23
5.2.4	Routing Hinweise .....	23
5.2.5	Secure-NTP (für GINO).....	24
5.2.6	Kartenleserverwaltung .....	24
5.2.7	OCSP .....	24
5.2.8	Applikationen und Services.....	24
5.2.9	GINA-IP vs. Client-IP / Anschluss-IP – MyIP Auskunftsservice.....	25
<b>5.3</b>	<b>Nating von LAN-CCRs und CCS .....</b>	<b>26</b>
5.3.1	NAT und GINO.....	26

## 1 Einleitende Informationen

Dieses Dokument soll einen kurzen Überblick über die Architekturumstellung im e-card System und den Connectivity Check bieten. Ein Großteil der hier zusammengefassten Informationen findet sich in diversen Dokumentationen bzw. wurde bereits bei den SWH Infoboards seitens SVC vermittelt.

### 1.1 Vorgehensweise für IT-Betreuer

Als IT-Betreuer haben sie möglicherweise den Auftrag eines Arztes, Apothekers, sonstigen VP (Vertragspartner) oder ELGA GDA (Gesundheitsdiensteanbieter) erhalten, sein Netzwerk zu prüfen.


„Wenn das e-card System aktuell genutzt werden kann, warum sind dann überhaupt Anpassungen notwendig?“ – Die Antwort darauf finden Sie in diesem Dokument.

Kurz zusammengefasst: für die aktuelle Nutzung ist es ausreichend, wenn die IP-Adresse der GINA vom Kartenleser und Rechner aus netzwerktechnisch erreicht wird. Nach Wegfall der GINA muss zum einen die DNS-Auflösung funktionieren und zum anderen müssen ganze Subnetze über den „e-card Router“ geführt werden.

Einen schnellen Überblick über die notwendigen Einstellungen finden Sie in [Kapitel 5 Allgemeine Hinweise zum VP-Netzwerk](#).

Stammt die Info, dass Handlungsbedarf besteht, von einer Fehlermeldung der e-card Web-Oberfläche, so enthalten die Kapitel [4.1.3](#) und [4.1.4](#) weiterführende Hinweise.

Beispiel einer e-card Web-Oberfläche Fehlermeldung:

V21.2.3.16Z /	/ Testsystem	 (008)	
Dr. Helga Musterärztin MSc			VPNR:044561
1020 Wien, Ernst-Melchior-Gasse 22 / Arzt			StNr:99 FG:01
23.11.2021			<a href="#">(H)ilfe</a>
<b>Anwendungsmenü</b>			
<b>Das GINS konnte nicht erreicht werden, um den Verbindungsstatus Ihres aktuell gewählten Kartenlesegeräts Reader0 (02:3c:a2) zu speichern. Die Erreichbarkeit des GINS ist zukünftig Voraussetzung zur Nutzung des e-card Systems. Bitte kontaktieren Sie Ihren IT-Betreuer! (CL-01140)</b>			
<b>(K)onsultationsverwaltung (KONV) starten</b>			

Den Erfolg gesetzter Maßnahmen können Sie mit den Methoden testen, die [in Kapitel 4.2 Manuelle Testmöglichkeiten](#) beschrieben sind.

Sollten nach Durchsicht dieses Dokuments bzw. der Dokumentation auf <https://www.chipkarte.at/gins> noch Fragen offen sein, wenden Sie sich bitte per Mail an [support@svc.co.at](mailto:support@svc.co.at)

### 1.2 Unterlagen und weitere Dokumentationen

Grundlegende Informationen zur Architekturumstellung werden halbjährlich im Zuge der SVC Infoboards präsentiert. Informationen zu den aktuellsten Infoboards finden Sie unter:

→ <https://www.chipkarte.at/infoboard>

Die Unterlagen weiter zurückliegender ASWH-Infoboards können unter folgendem Link eingesehen werden:

→ <https://www.chipkarte.at/cdscontent/?contentid=10007.759497&portal=ecardportal>

Informationen zur Implementierung mittels SS12 können aus der Schnittstellenbeschreibung (JavaDoc) der aktuellen e-card Release bezogen werden:

→ [www.chipkarte.at](http://www.chipkarte.at)

Die Dokumentation zur REST-API des Connectivity Check Service (CCS) und Card Reader Service (CRS) befindet sich unter

→ <https://www.sozialversicherung.at/de/ecard/swagger-ui/ss92/>

In den Downloadbereichen für Arztsoftware-, Apotheken- und WGDA-SW-Hersteller, sowie im Bereich für Hersteller von Krankenhausinformationssystemen finden Sie die aktuellen SoapUI Beispielprojekte für KSE bzw. VDAS, welche exemplarisch die notwendigen Funktionsaufrufe im Rahmen des CCS enthalten.

Eine Übersicht, über die notwendigen Firewall- und Portkonfigurationen, speziell in Krankenanstalten<sup>1</sup>, findet sich auf →

<https://www.chipkarte.at/cdscontent/?contentid=10007.678628&portal=ecardportal#FirewallundPortkonfigurationbr678628>

Eine genaue Beschreibung der Anforderungen an das VP-Netzwerk findet sich im Netzwerkdokument GINS unter

<https://www.chipkarte.at/gins>

<https://www.chipkarte.at/cdscontent/load?contentid=10008.753737&version=1634293727>

Information zu den zu installierenden Zertifikaten findet sich unter

<https://www.chipkarte.at/zertifikate>

---

<sup>1</sup> Teile dieser Information gelten auch für „herkömmliche“ GIN-Anschlüsse.  
CCS Kurzanleitung

## 2 Allgemeine Informationen

### 2.1 Big Picture / Motivation

Um zu verstehen, warum es den Connectivity Check braucht und um die einzelnen Aspekte der Tests besser nachvollziehen zu können, ist es notwendig ein Verständnis dafür zu entwickeln, wie sich die Umstellung der Systemarchitektur auswirkt.

Die Umstellung erstreckt sich im Wesentlichen auf zwei Bereiche:

- **Software-Umstellung**  
Betrifft zum einen die Umstellung der e-card Services und deren Arbeitsweise durch die SVC und die Einführung des GINS (Gesundheits-Informations-Netz-Services) und die damit verbundene Art und Weise wie die Vertragspartner-Software diese Services nutzt.
- **Hardware-/Netzwerkumstellung**  
Mit der Software-Umstellung und der Einführung von GINS gehen auch geänderte Anforderungen an das LAN des VP einher. Werden diese Anforderungen nicht erfüllt, ist ein Weiterarbeiten nach dem Hardware-Tausch (Abbau der GINA und Tausch LAN-CCR gegen GINO) nicht möglich.  
Das CCS (Connectivity Check Service) ermöglicht es, diese Anforderungen zu testen.

#### 2.1.1 Software-Umstellung

Die Software-Umstellung betrifft die Implementierung bzw. Funktionsweise der einzelnen e-card Services, sowie die Nutzung durch die VP-Software. Beginnend mit dem 32. Infoboard zum R18a Release (Frühjahr 2018) wurde diese Umstellung in jeder Informationsveranstaltung ausführlich behandelt<sup>2</sup>.

- a. **„cardReaderId“-Services mit Client-Verarbeitung auf der GINA**  
Bei herkömmlichen Services wurde der Request auf der GINA einer Client-Verarbeitung unterzogen und danach in komprimierter Form ans e-card Zentralsystem weitergeschickt. Funktionen dieser Services verfügen noch über die `cardReaderId` als Input-Parameter. Die VP-SW kommuniziert dabei direkt mit der GINA;  
→ Beispiel: VDAS Version 15  
<https://10.134.240.17/vdas/15>
- b. **„cardToken“-Services wahlweise mit Client-Verarbeitung oder Proxy-Modus**  
Services, die bereits auf „cardToken“ anstatt „cardReaderId“ als Parameter umgestellt wurden, können entweder mit Client-Verarbeitung auf der GINA betrieben werden oder im „Proxy-Modus“<sup>3</sup>. In der Proxy-Variante leitet die GINA die SOAP-XML Requests 1:1 ans e-card Rechenzentrum weiter, die SOAP-XML Antwort wird dort generiert und 1:1 via GINA an die VP-SW zurückgeliefert.  
Die Umstellung zwischen den beiden Modi kann von der VP-SW nicht beeinflusst werden. Sie wird per Konfiguration seitens SVC aktiviert oder deaktiviert.

---

<sup>2</sup> Zurückreichend bis zum 33. Infoboard (R18b) sind die Präsentationen auf [www.chipkarte.at](http://www.chipkarte.at) noch zum Download bereitgestellt.

<sup>3</sup> Die Implementierung der zwei Varianten „Client-Verarbeitung“ und „Proxy-Modus“ mit zentraler Verarbeitung gilt für alle bestehenden Services. Neu hinzukommende Services (wie z.B. REZ oder MUHI) werden nur noch in der zentralen Variante mit Proxy-Modus implementiert.

In beiden Varianten kommuniziert die VP-SW direkt mit der GINA.

→ Beispiel: VDAS Version 16

<https://10.134.240.17/vdas/16>

c. GINS (Gesundheits-Informations-Netz-Services)

GINS bezeichnet die zentrale Servicenutzung ohne Beteiligung der GINA. Die VP-SW kommuniziert in dieser Variante per „Hostnamen“<sup>4</sup> mit dem Zentralsystem „an der GINA vorbei“ direkt über den e-card Router. Nach dem Wegfall der GINA und dem Tausch LAN-CCR gegen GINO wird diese Nutzungsvariante die einzig mögliche sein.

Die VP-SW kann die Nutzung der GINS steuern, indem der „zentrale Servicemanager“ abgefragt wird und somit die entsprechenden QoS (Quality of Service) Hostnamen verwendet werden.

GINS ist in der Testumgebung derzeit bereits nutzbar und wird in der Produktionsumgebung gegen Ende des Jahres 2021 verfügbar sein.

→ Beispiel: VDAS Version 16

<https://services-a.ecard-test.sozialversicherung.at:443/vdas/16><sup>5</sup>

## 2.1.2 Hardware-/Netzwerkumstellung

### 2.1.2.1 Status Quo Netzwerkerreichbarkeit

Derzeit ist der GIN-Adapter – kurz GINA – der zentrale Punkt, an dem die Kommunikation von VP-SW, Kartenleser und e-card Serversystem zusammentrifft.

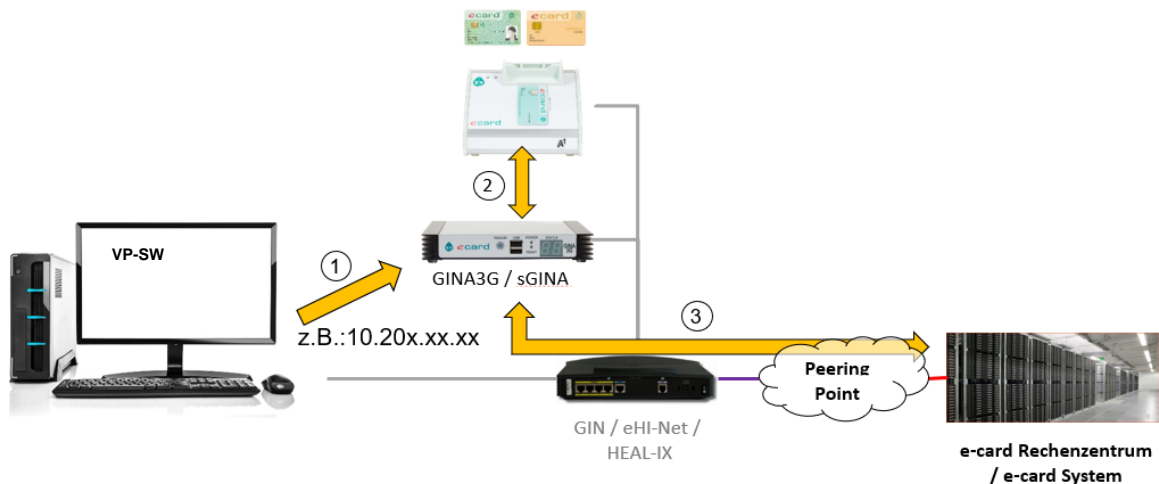


Abbildung 1: Abstrahierte Kommunikationswege (Status Quo)

<sup>4</sup> Selbstverständlich werden diese Hostnamen auf IP-Adressen übersetzt. Aber es wird dringend davon abgeraten, auf eine DNS-Auflösung zu verzichten und direkt mit den entsprechenden IP-Adressen zu kommunizieren, da sich diese im vorgesehenen Adressbereich ohne Rücksprache ändern können.

<sup>5</sup> Der Service-Endpoint bezieht sich auf das Testsystem. In Produktion lautet der entsprechende Endpoint für VDAS Version 16: <https://services.ecard.sozialversicherung.at:443/vdas/16> (Die Angabe des Ports 443 für https ist optional.)

Stark abstrahiert<sup>6</sup> gesprochen müssen aktuell auf Netzwerkebene folgende Bedingungen für eine funktionierende Installation gewährleistet sein:

1. Die VP-SW muss die GINA-IP erreichen können.  
Bei mehr als einem Router im VP-LAN wäre es derzeit ausreichend, wenn nur die GINA-IP an den e-card Router weitergeroutet wird.
2. Die GINA muss den Kartenleser erreichen können.  
Derzeit ist keine direkte Netzwerkerreichbarkeit zwischen Kartenleser und VP-Software notwendig (auch wenn der LAN-CCR Adapter für das Auslesen der Karte und Generieren der Token verwendet wird).
3. Die GINA muss das e-card Zentralsystem erreichen können.  
(Siehe Skizze)

### 2.1.2.2 Netzwerkerreichbarkeit mit GINS

Nach dem Wegfall der GINA und dem Tausch LAN-CCR gegen GINO sind die folgenden Änderungen bezüglich Erreichbarkeit im Netzwerk zu beachten.

Die entsprechenden Vorbedingungen werden hier überblicksmäßig dargestellt. Im Laufe des Q3 2021 wird zum Thema Netzwerkkonfiguration und Routing noch ein separates Dokument seitens SVC erstellt und veröffentlicht.

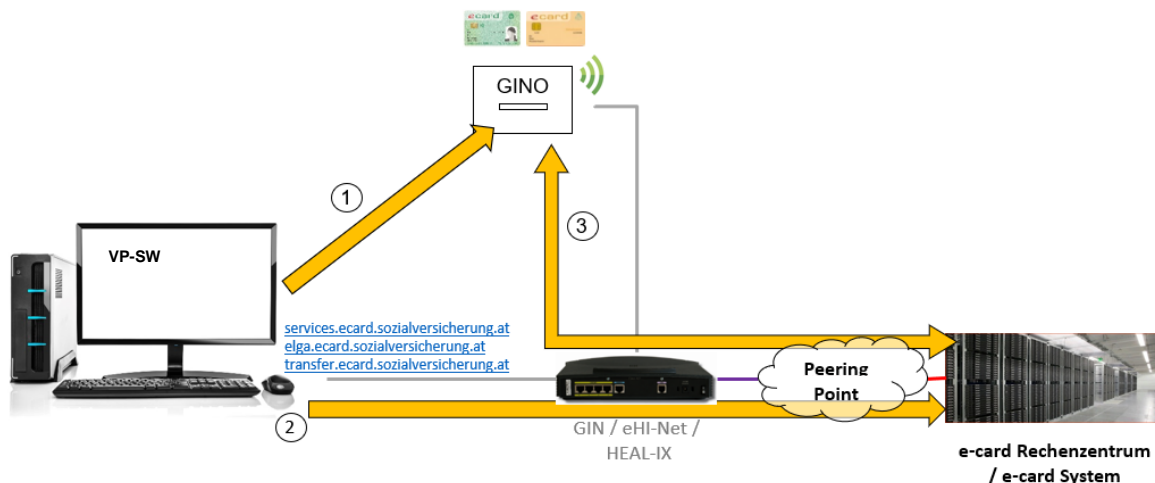


Abbildung 2: Abstrahierte Kommunikationswege bei GINS-Nutzung

1. Direkte Erreichbarkeit des GINOs durch die VP-SW  
Netzwerktechnisch muss sichergestellt sein, dass eine direkte Kommunikation möglich ist.

CCS-Test:

http GET auf die „checkIp“, welche vom CRS zurückgeliefert wird. Details siehe [Direkte Erreichbarkeit des LAN-CCR aus VP-SW prüfen](#)

2. Direkte Erreichbarkeit des GINS (e-card Zentralsystem) durch die VP-SW  
Es muss sichergestellt sein, dass die QoS Hostnamen per DNS<sup>7</sup> korrekt aufgelöst werden

<sup>6</sup> Die Skizze in Abbildung 1 ist vereinfacht dargestellt. Der Kartenleser befindet sich z.B. im Adressbereich des VP-LANs und nicht im Adressbereich der GINA. Auch wenn in Produktion die Installationsvariante mit einem zweiten Router im VP-Netzwerk häufig vertreten ist, wurde darauf in der Skizze keine Rücksicht genommen.

<sup>7</sup> Idealerweise ist hier der Peering Point / e-card DNS mit 84.38.113.161 oder 84.38.113.162 eingetragen.  
CCS Kurzanleitung

können.

Zusätzlich ist es notwendig, dass die zugeordneten IP-Adressen über den e-card Router weitergeleitet werden. Dazu ist zumindest für den folgenden Adressbereich eine entsprechende Route einzutragen:

84.38.112.0/20

CCS-Test:

Erfolgreicher zweimaliger<sup>8</sup> Aufruf der `/check` oder `/checkDetails` Ressource des CCS. Da dieses Service nicht über die GINA-IP angesprochen werden kann, ist ein erfolgreicher Aufruf mit der Erreichbarkeit des GINS gleichzusetzen.

Hinweis: Dieser Test sollte auf jeder Arbeitsstation durchgeführt werden, die e-card Services nutzt (mit oder ohne zugeordnetem Kartenleser).

3. Direkte Erreichbarkeit des GINS (e-card Zentralsystem) durch den Kartenleser  
Der GINO muss in der Lage sein das Zentralsystem direkt erreichen zu können. Wie beim Rechner der VP-SW unter Punkt 2 muss auch der Kartenleser in der Lage sein, die QoS Hostnamen per DNS auflösen zu können und im Netzwerk muss sichergestellt sein, dass das entsprechende Routing zum e-card Router eingetragen ist:

84.38.112.0/20

CCS-Test:

In Vorbereitung auf den GINO, wird die Erreichbarkeit des GINS durch einen „Selbsttest“<sup>9</sup> des LAN-CCRs automatisch geprüft. Die Ergebnisse dieses Tests können mittels der `/checkDetails` Ressource des CCS abgerufen werden.

---

<sup>8</sup> Die `/check` bzw. `/checkDetails` Ressource soll einmal per http und einmal per https aufgerufen werden; per https um sicher zu gehen, dass ausreichend „starke“ Kryptoalgorithmen unterstützt werden und http damit die Information, welcher DNS die Namensauflösung durchgeführt hat, transportiert und zurückgeliefert werden kann – der Peering Point oder ein „öffentlicher“ DNS.

<sup>9</sup> In der Testumgebung führt der LAN-CCR den „Selbsttest“ bereits seit Mitte April 2021 durch. In Produktion wurde dieser Ende Juni 2021 aktiviert.  
CCS Kurzanleitung



## 3 Kurzanleitung zur CCS Implementierung

Grundsätzlich empfehlen wir, den Connectivity Check einmal pro Tag im Rahmen des Dialogaufbaus durchzuführen. Um diesen Check auch VPs zu ermöglichen, welche die Web-Oberfläche nutzen, wird dieser Test auch von der Web-Oberfläche im Zuge des Dialogaufbaus durchgeführt.

Aus Sicht der VP-SW teilt sich der Connectivity Check in zwei Bereiche:

- Prüfen der Erreichbarkeit des GINS und Hochladen<sup>10</sup> der Information, ob die Kartenleser direkt erreichbar sind, mittels der CCS Ressource `/check`
- Abfragen der „Selbsttest“ Information des Kartenlesers mittels der CCS Ressource `/checkDetails`

### 3.1 Erreichbarkeit des GINS prüfen

#### 3.1.1 Überblick Vorgehensweise

Die Erreichbarkeitsprüfung des GINS via CCS gliedert sich in folgende Schritte:

1. Prüfung, ob CCS bereits verfügbar ist ([3.1.2.1](#))
2. Endpoint-URLs für CCS abfragen ([3.1.2.2](#))
3. `checkIp's` der Kartenleser abfragen ([3.1.2.3](#))
4. Direkte Erreichbarkeit des LAN-CCR aus VP-SW prüfen ([3.1.2.4](#))
5. GINS Erreichbarkeit prüfen, inkl. Konnektivität des LAN-CCR übermitteln ([3.1.2.5](#))

Die Schritte 4 und 5 sollen von jeder Arbeitsstation aus durchgeführt werden. Um die Anzahl der Requests ans GINS geringer zu halten, kann die Übermittlung der Konnektivitätsinformation zu den LAN-CCRs auch nur auf einer Station und für einen QoS Endpunkt erfolgen.

#### 3.1.2 Vorgehensweise Details

##### 3.1.2.1 Prüfung, ob CCS bereits verfügbar ist

Durch Aufruf der Funktion `connectivityCheckAvailable()` des GINA-Service.

Sobald der Connectivity Check produktiv zur Verfügung steht, wird dieser Funktionsaufruf „true“ zurückliefern.

##### 3.1.2.2 Endpoint-URLs für CCS abfragen

Der Aufruf der Funktion `getServices()` des Service-Managers<sup>11</sup> liefert die verfügbaren Services und deren Endpoints zurück. Für das CCS werden 3 Einträge für die 3 unterschiedlichen Quality of Service (QoS) Stufen zurückgeliefert.

---

<sup>10</sup> Das Hochladen der Information, ob ein ausgewählter Kartenleser von der VP-SW direkt erreicht werden kann, ist im Request optional, sollte aber zumindest auf einer Station durchgeführt werden.

<sup>11</sup> In diesem Zusammenhang ist der „lokale“ Servicemanager gemeint, der über die GINA-IP erreichbar ist. Der „zentrale Servicemanager“ (Aufruf über den „services“ QoS Hostname) ist derzeit nur in der Testumgebung verfügbar. In Produktion wird dieser ab Ende 2021 verfügbar sein.

Testumgebung:

QoS	Name	endPointURL
hoch	ccs_services	<a href="https://services-a.ecard-test.sozialversicherung.at/ccs/1">https://services-a.ecard-test.sozialversicherung.at/ccs/1</a>
mittel	ccs_elga	<a href="https://elga-a.ecard-test.sozialversicherung.at/ccs/1">https://elga-a.ecard-test.sozialversicherung.at/ccs/1</a>
niedrig	ccs_transfer	<a href="https://transfer-a.ecard-test.sozialversicherung.at/ccs/1">https://transfer-a.ecard-test.sozialversicherung.at/ccs/1</a>

Produktion:

QoS	Name	endPointURL
hoch	ccs_services	<a href="https://services.ecard.sozialversicherung.at/ccs/1">https://services.ecard.sozialversicherung.at/ccs/1</a>
mittel	ccs_elga	<a href="https://elga.ecard.sozialversicherung.at/ccs/1">https://elga.ecard.sozialversicherung.at/ccs/1</a>
niedrig	ccs_transfer	<a href="https://transfer.ecard.sozialversicherung.at/ccs/1">https://transfer.ecard.sozialversicherung.at/ccs/1</a>

Diese URLs haben die GINA-IP nicht als Bestandteil. Daher müssen für einen funktionierenden Check diese Hostnamen

- per DNS aufgelöst werden können und
- die aufgelöste IP über den e-card Router aus dem lokalen VP-LAN „geschickt“ werden.  
(Die Route für 84.38.112.0/20 muss über den e-card Router führen.)

### 3.1.2.3 checkIp's der Kartenleser abfragen

Beim Aufruf der /readers Ressource des Card Reader Service (CRS) werden alle dem Anschluss zugeordneten Kartenleser zurückgeliefert.

Aus der Response sind für das CCS die folgenden Parameter relevant:

- checkIp (lokale IP-Adresse des Kartenlesers) → Input Parameter lanccrIp für CCS
- id (ID des Kartenlesers) → Input Parameter lanccrId für CCS

### 3.1.2.4 Direkte Erreichbarkeit des LAN-CCR aus VP-SW prüfen

Die direkte Erreichbarkeit der Kartenleser wird mittels „http GET“<sup>12</sup> auf die IP jedes einzelnen Kartenlesers

„http://[checkIp]“<sup>13</sup>  
geprüft.

Erwartetes Ergebnis:

http Status Code 301 „moved permanently“

Je nach verwendetem Framework oder Tool ist es notwendig, den automatischen http Redirect zu deaktivieren (redirect=false). Ansonsten wird automatisch zu https weitergeleitet.

Der Zweck dieses Checks ist es, zu prüfen, ob nach der Hardwareumstellung direkt mit den GINOs kommuniziert werden kann. Die Annahme ist, dass diese netzwerktechnisch gleich installiert werden, wie jetzt die LAN-CCRs.

<sup>12</sup> Falls das für den Check verwendete Framework über eine Einstellung verfügt, die automatisch einem http Redirect auf https folgt, ist diese zu deaktivieren, um das gewünschte Ergebnis „http Status Code 301“ zu bekommen.

<sup>13</sup> [checkIp] ist hier als Platzhalter für die tatsächliche IP-Adresse des LAN-CCRs gewählt (Parameter checkIp aus CRS Response).

**Ergebnisübermittlung:**

Das Ergebnis der Prüfung ist im Aufruf der CCS Ressource `/check` oder `/checkDetails` im Parameter `lanccrErreichbar` zu übermitteln.

Für den Test aus der VP-SW heraus sollte die direkte Verbindung von jeder Station zu den jeweiligen Kartenlesern getestet werden. Für die Übermittlung per CCS ist es grundsätzlich ausreichend, wenn die entsprechenden Werte pro Kartenleser nur einmal pro Tag von einer ausgewählten Station<sup>14</sup> übermittelt werden.

**Verhalten bei vielen LAN-CCRs:**

Die lokale Verbindungsprüfung aus der VP-SW heraus muss im Eigeninteresse für jeden Kartenleser durchgeführt werden. Genauer gesagt, sollte dieser Test auf jeder Station für die dort potentiell verwendbaren Kartenleser erfolgen.

Da aber die Übermittlung der Kartenleser-Erreichbarkeitsinformation primär statistischen Zwecken dient, kann im Sinne der Begrenzung der Funktionsaufrufe bei mehr als fünf Lesern auf folgende Vereinfachung<sup>15</sup> zurückgegriffen werden:

- Aus allen direkt erreichbaren Kartenlesern einen auswählen und für diesen die Information `lanccrErreichbar:true` übertragen.
- Aus allen nicht erreichbaren Kartenlesern einen auswählen und für diesen die Information `lanccrErreichbar:false` übertragen.

Damit kann zentral erfasst werden, ob bei dieser Installation im Vorfeld der Umstellung noch Anpassungsbedarf besteht.

**3.1.2.5 GINS-Erreichbarkeit prüfen (inkl. Konnektivität des LAN-CCR übermitteln)**

Der Aufruf der `/check` Ressource dient zwei Zielen:

- GINS-Erreichbarkeit prüfen
- Kartenleserinformation übermitteln

**GINS-Erreichbarkeit prüfen:**

Auf jeder Station, welche e-card Services verwendet, muss die `/check` Ressource aufgerufen werden um zu prüfen, ob ein Call „an der GINA vorbei“ möglich ist und somit auch nach der Hardwareumstellung mit dem GINS kommuniziert werden kann.

Jeder der drei QoS Endpoints (`services`, `elga` und `transfer`) soll dabei einmal per `http` und einmal per `https` aufgerufen werden.

Wie schon erwähnt, ist es für einen funktionierenden Check wesentlich, dass die DNS-Auflösung der drei Hostnamen funktioniert, sowie das Routing für die aufgelösten IP-Adressen über den e-card Router führt.

Der Aufruf per `https` ist wichtig um zu prüfen, ob die notwendigen Kryptoalgorithmen für die verschlüsselte Verbindung unterstützt werden. Der Aufruf per `http` ist wichtig, um die Information zu transportieren, welcher DNS für die Namensauflösung verwendet wurde.

---

<sup>14</sup> Es steht dem SW-Hersteller frei, die Kartenleser-Erreichbarkeitsinformationen von jeder Station aus per CCS ans e-card System zu übermitteln. Im Sinne einer Reduktion der notwendigen Funktionsaufrufe sollte aber auf eine redundante Übermittlung der Ergebnisse verzichtet werden.

<sup>15</sup> Liefern die Tests von unterschiedlichen Stationen widersprüchliche Ergebnisse, so soll das „schlechtere“ Ergebnis übermittelt werden; z.B.: Kartenleser „lanccr A (12:23:45)“ wird potentiell von zwei Stationen verwendet. Liefert der Erreichbarkeitstest aber nur auf einer Station ein positives Ergebnis, so ist `lanccrErreichbar:false` zu übertragen.

Erwartete Ergebnisse:

- http-Aufruf → 200 „OK“ + Information ob öffentlicher DNS verwendet wurde (false) oder der Peering Point DNS zur Anwendung kam (true)
- https-Aufruf → 204 „No Content“ → es wird keine Information über den verwendeten DNS retourniert

Rein aus dem Blickwinkel des GINS-Erreichbarkeitstests sind also einmal täglich pro Arbeitsstation sechs Funktionsaufrufe per CCS notwendig.

#### **Kartenleserinformation übermitteln:**

Wie in Kapitel [3.1.2.4](#) beschrieben, soll einmal pro Tag auf einer ausgewählten Station per `/check` Ressource die Information übermittelt werden, ob die verwendeten Kartenleser direkt aus der VP-SW erreicht werden können oder nicht. Die Information wird dadurch übertragen, dass zusätzlich zum verpflichtenden Parameter

- `vpnr`

auch die optionalen Parameter

- `lanccrId`
- `lanccrIp` und
- `lanccrErreichbar`

übermittelt werden.

Diese Information muss aber nur für einen QoS Hostnamen und nur über ein Protokoll (http / https) übertragen werden.

Für eine konsistente Ergebnisauswertung empfehlen wir, die Erreichbarkeitsinformation für die höchste QoS Stufe (services) und per https zu übertragen.

#### **Beispiel:**

Bei einer Installation mit drei Stationen:

- Aufnahme
- Behandlung 1
- Behandlung 2

und zwei Kartenlesern:

- `lanccr aufnahme(12:34:56)`
- `lanccr arzt (23:45:67)`

kann die Informationsübermittlung per CCS zum Beispiel folgendermaßen aussehen:

1x pro Tag

- Station Aufnahme
  - 2 Aufrufe des „services“ Endpoints per https (jeweils für `lanccr aufnahme` und `lanccr arzt`)
  - 1 Aufruf des „services“ Endpoints ohne Kartenleser-Information (http)
  - 2 Aufrufe des „elga“ Endpoints ohne Kartenleser-Information (http + https)
  - 2 Aufrufe des „transfer“ Endpoints ohne Kartenleser-Information (http + https)
- Station Behandlung 1 und Behandlung 2 – jeweils:
  - 2 Aufrufe des „services“ Endpoints ohne Kartenleser-Information (http + https)
  - 2 Aufrufe des „elga“ Endpoints ohne Kartenleser-Information (http + https)
  - 2 Aufrufe des „transfer“ Endpoints ohne Kartenleser-Information (http + https)

Hinweis: Alternativ kann die Übermittlung der Kartenleser-Erreichbarkeit jeweils auf der Station, wo dieser eingebunden ist oder auf jeder Station für alle Kartenleser erfolgen.

### 3.2 Ergebnisabfrage des Kartenleser-„Selbsttests“

Neben der Erreichbarkeit des GINS und der direkten Erreichbarkeit der Kartenleser aus der VP-SW heraus, ist es notwendig, dass auch die Kartenleser selbst direkt das GINS erreichen können. Diese Bedingung wird von den Kartenlesern mittels „Selbsttest“ geprüft.

Die Ergebnisse dieses Tests können mit der Ressource `/checkDetails` des CCS abgefragt werden. Für die VP-SW ist es wichtig, diese Abfrage ebenfalls durchzuführen, da ohne der direkten Erreichbarkeit des GINS durch den Kartenleser die GINOs nach dem Hardwaretausch nicht arbeiten können.

Mit R21a wurde dem CCS die Ressource `/checkDetails` hinzugefügt.

Anders als bei `/check` ist hier die Angabe der `lanccrIp`<sup>16</sup> und `lanccrId` zwingend erforderlich.

Die Response-Parameter sind:

- `ntpsErreichbar`: Info ob NTP erreichbar ist  
true → OK  
false → Handlungsbedarf
- `sshsErreichbar`: Info ob SSH erreichbar ist  
true → OK  
false → Handlungsbedarf
- `kalveErreichbar`: Info ob die Kartenleserverwaltung erreichbar ist  
true → OK  
false → Handlungsbedarf
- `ocspErreichbar`: Info ob der Zertifikatsserver erreichbar ist  
true → OK  
false → Handlungsbedarf
- `lastConnection`: letzter erfolgreicher Verbindungsaufbau dieses Kartenlesers mit dem GINS (dd.mm.yyyy)
- `lanccrErreichbar`: Info, ob der Kartenleser aus der VP-Software direkt erreichbar ist. (Das ist der letzte übermittelte Wert von `/check` oder `/checkDetails` für diesen Kartenleser.)
- `ppDnsServer`: Info, ob der e-card DNS oder ein öffentlicher DNS verwendet wurde (wird nur bei Aufrufen per http retourniert)  
true → e-card DNS  
false → öffentlicher DNS → eventuell Handlungsbedarf: e-card DNS<sup>17</sup> als primären DNS eintragen

---

<sup>16</sup> Hinweis: Hier sollte die reale, lokale IP-Adresse des Kartenlesers angegeben werden (keine NAT-IP). Der Kartenleser meldet sich im Zuge des Selbsttests mit seiner lokalen IP-Adresse beim CCS.

<sup>17</sup> 84.38.113.161 oder 84.38.113.162 (für Testumgebung und Produktion)  
CCS Kurzanleitung

## 4 Fehlerbehandlung/Ergebnisauswertung

Wie im 38. Infoboard zu R21a angekündigt, sollte in einem ersten Schritt der Connectivity Check implementiert werden. Es ist geplant, im Juli und August 2021 nach dem Aktivieren des CCS erste Ergebnisse zu sammeln und auszuwerten.

Eine Anzeige möglicher negativer Ergebnisse durch die VP-SW sollte dann idealerweise erst nach Information seitens SVC ab 20.09.2021 erfolgen. Am 16.09.2021 findet/fand dazu eine Informationsveranstaltung statt.

Eine genaue, aktualisierte Beschreibung der notwendigen Netzwerkstruktur beim VP bzw. Hinweise zur Anpassung und Fehlerbehebung wird gesondert erfolgen.

### 4.1 Mögliche Ursachen bei fehlschlagenden Tests

Derzeit erstrecken sich die Tests auf die Testumgebung. In Produktion wurde das Connectivity Check Service Anfang Juli 2021 freigeschaltet. Die Problembeseitigung in Produktion und Testumgebung ist im Grunde ident.

Die bisherige Analyse der CCS-Ergebnisse seitens SVC hat gezeigt, dass in 99% der Fälle, wo der Aufruf des CCS das e-card System erreichen konnte, alle Tests (LAN-CCR-Erreichbarkeit, NTP, SSH, etc.) erfolgreich waren. Daraus lässt sich ableiten, dass nicht Firewall-Einstellungen für einzelne Ports, sondern das generelle Routing die Hauptursache für fehlschlagende Tests darstellt.

#### 4.1.1 Aufruf der /check oder /checkDetails Ressource schlägt fehl

##### **Prüfen, ob die DNS-Auflösung funktioniert:**

Testumgebung:

Der Hostname  
services-a.ecard-test.sozialversicherung.at  
muss auf  
84.38.112.28 (e-card DNS) oder  
84.38.112.29 („Internet“ DNS)  
aufgelöst werden.

Produktion:

Der Hostname  
services.ecard.sozialversicherung.at  
muss auf  
84.38.112.30 (e-card DNS) oder  
84.38.112.31 („Internet“ DNS)  
aufgelöst werden.

##### **Prüfen, ob Routing funktioniert:**

Funktioniert die Namensauflösung, liegt ein fehlschlagender Aufruf eventuell am Routing im lokalen Netzwerk. Es lösen zwar sowohl der e-card DNS als auch ein öffentlicher DNS die jeweiligen Hostnamen auf, die Ziel-IP ist aber in beiden Fällen eine IP im e-card Netz.

Wird der Aufruf also über ein Standard-Gateway ins „Internet“ geschickt, schlägt der Call fehl. Die Route für 84.38.112.0/20 muss über den e-card Router führen.

##### **Verschlüsselungsfehler beim Aufruf:**

Die notwendigen Zertifikate für die Kommunikation mit GINS und der lokalen GINA leiten sich von derselben Hierarchie ab.

In Einzelfällen gab es Probleme mit veralteten TLS Algorithmen (z.B. TLS 1.0), die für die Kommunikation mit GINS nicht mehr unterstützt werden.

Zur Prüfung, ob die verschlüsselte Kommunikation grundsätzlich funktioniert, kann auf die aktuellen KSE bzw. VDAS SoapUI-Projekte zurückgegriffen werden, welche den Connectivity Check bereits implementiert haben.

#### 4.1.2 Aufruf von /checkDetails liefert keine Information zum Kartenleser

/checkDetails liefert dann eine Information zurück, wenn der Kartenleser-Selbstcheck das GINS erreichen konnte. Beim „Selbsttest“ verwendet der Kartenleser die gleichen CCS Hostnamen wie die VP-SW. Demnach gilt auch für den Kartenleser, dass die Namensauflösung und das Routing im lokalen Netzwerk funktionieren müssen.

Bei statisch konfigurierten Kartenlesern kann es sein, dass die DNS-IP leer ist oder eventuell einen ungültigen Wert<sup>18</sup> hat.

In der Testumgebung wurden alle Kartenleser per Script seitens SVC so konfiguriert, dass bei statischer Konfiguration und leerem DNS die Adresse den Peering Point DNS ( 84.38.113.161) eingetragen wurde.

Sollten Sie von /checkDetails ein leeres Ergebnis zurückbekommen, prüfen Sie bitte die Einstellungen beim Kartenleser im Admin-Menü desselben.

#### 4.1.3 Fehlermeldungen bei Nutzung der Web-Oberfläche und mögliche Behebung

Mit Release R21b und der Umstellung der Web-Oberfläche mit 24.11.2021 bzw. 1.12.2021 sind die angezeigten Fehlermeldungen detaillierter:

Fehler-Nr.	Fehlermeldung	Beispiele für mögliche Fehlerursachen
CL-01140	Das GINS konnte nicht erreicht werden, um den Verbindungsstatus Ihres aktuell gewählten Kartenlesegeräts {0} zu speichern. Die Erreichbarkeit des GINS ist zukünftig Voraussetzung zur Nutzung des e-card Systems. Bitte kontaktieren Sie Ihren IT-Betreuer!	<p>Das Gesundheitsinformationsnetz-Service (GINS) konnte nicht erreicht werden. → z.B. der PC erreicht das GINS nicht (Services am Zentralsystem)</p> <p>Möglicherweise kann der LAN-CCR die Daten übertragen (siehe Testdetails<sup>19</sup>)</p> <p>Der IT-Betreuer sollte hier alle Tests (DNS, Routing, ...) <b>auf den PC</b> richten, das Gesamtnetzwerk dabei aber natürlich nicht außer Acht lassen. Ein manueller Aufruf der Test-URLs im GIN wird auch empfohlen.</p>
CL-01141	Ihr gewähltes Kartenlesegerät {0} konnte das GesundheitsInformationsNetzService (GINS) nicht erreichen. Die Erreichbarkeit des GINS ist zukünftig Voraussetzung zur Nutzung des e-card Systems. Bitte kontaktieren Sie Ihren IT-Betreuer!	<p>Der Kartenleser hat sich nicht beim GINS gemeldet.</p> <p>Der IT-Betreuer sollte alle Tests (DNS, Routing, manueller Aufruf der Test-URLs im GIN, ...) mit dem Fokus auf das ganze Netzwerk beginnen.</p>

<sup>18</sup> Für das Funktionieren eines Kartenlesers im Zusammenhang mit der GINA ist es nicht zwingend erforderlich, dass der DNS beim Kartenleser (korrekt) eingetragen ist.

<sup>19</sup> Die Web-Oberfläche bietet die Möglichkeit zur Anzeige der letzten Prüfungsergebnisse des gewählten LAN-CCRs an (siehe „(I)nformationsdienste“ / „Verbindungsstatus des aktuell gewählten (K)artenlesegeräts anzeigen“)  
CCS Kurzanleitung



CL-01142	Ihr gewähltes Kartenlesegerät konnte das GesundheitsInformationsNetzService (GINS) seit {0} Tagen nicht erreichen. Bitte kontaktieren Sie Ihren IT-Betreuer!	Normalerweise kontaktiert der LAN-CCR das Zentralsystem täglich. Was hat sich verändert?
CL-01143	Der Verbindungsstatus Ihres aktuell gewählten Kartenlesegeräts ist für mindestens eine Komponente negativ. Bitte kontaktieren Sie Ihren IT-Betreuer!	Bei der Kommunikation/Verbindung mit dem Kartenleser ist mindestens ein Problem aufgetreten.  Hier können die Detailinformationen helfen (siehe Fußnote 19 auf Seite 16). Der Fokus liegt auf einzelnen Teilen im Netzwerk, die hier vom Kartenleser aus nicht erreichbar sind.

#### 4.1.4 Weitere mögliche Fehlerursachen

- Die https-Root-Zertifikate im Browser fehlen**  
Die Verbindungstests zum Zentralsystem verwenden eine https-Verbindung. Wenn im Browser die entsprechenden Root-Zertifikate von [www.chipkarte.at/zertifikate](http://www.chipkarte.at/zertifikate) nicht installiert sind, kann die Verbindung durch das Script nicht verschlüsselt aufgebaut werden. Dadurch werden Verbindungsfehler angezeigt, die ähnlich aussehen können wie eine Nichterreichbarkeit des Zentralsystems durch ein Netzwerkproblem.
- Einspielen der https-Root-Zertifikate in der VPSWH-Umgebung unvollständig**  
Auch für die Prüfung in der Web-Oberfläche in der Testumgebung, ist die Installation der Test-UND Produktiv-Zertifikate notwendig. Die GINS Services arbeiten in der Testumgebung auch über die produktive Zertifikats-Prüfkette.
- Veraltete Betriebssysteme liefern GINS Prüfungsfehler**  
Da das Zentralsystem aus Sicherheitsgründen nur noch TLS 1.2 zur Verfügung stellt, können stark veraltet Betriebssysteme oder Browser keine sichere https-Verbindung zu den zentralen Services aufbauen (obwohl die Verbindung zur GINA funktioniert und die Zertifikate eingespielt sind). Ursache ist, dass in alten Browsern oder Betriebssystemen nur TLS 1.0 und TLS 1.1 angeboten werden. TLS 1.2 steht (bzw. stand damals) noch nicht zur Verfügung. Da TLS 1.0 und TLS 1.1 von Experten als unsicher angesehen werden, sind diese nicht mehr am Zentralsystem (GINS) zugelassen. Für Nutzer dieser stark veralteten Betriebssysteme sieht es in Folge nach einem Netzwerkfehler aus – ist aber ein Fehler, der womöglich durch ein nicht mehr unterstütztes Betriebssystem (oder Browser) verursacht wurde. Unterstützte Browser und Betriebssysteme finden Sie unter [www.chipkarte.at/ecs-browser](http://www.chipkarte.at/ecs-browser). Für eine Nutzung der zentralen Services benötigen Sie aktuelle und durch den Hersteller mit Updates versorgte Browser und Betriebssysteme. Die Unterscheidung, ob ein Betriebssystem oder Netzwerkeinstellungen das Problem verursachen, liegt vollständig im Kompetenzbereich des Softwareherstellers oder IT-Betreuers.
- Welche Zertifikate müssen eingespielt werden**  
In der Testumgebung (VPSWH) sind eigene, vom Produktivsystem abweichende Zertifikate auf der GINA in Verwendung. Die Besonderheit dabei ist, dass in der Testumgebung (bei den zentralen Services im GINS) die gleichen Zertifikatsketten wie in der Produktion verwendet werden. Das bedeutet (nur für die Testumgebung), dass sowohl den Test-, als auch den Produktions-Root Zertifikaten vertraut werden muss. Die fehlenden Produktions-Root-Zertifikate könnten zu Verbindungs-Aufbauproblemen bei den CCS Tests führen und irrtümlich als Netzwerkproblem eingeschätzt werden. Das betrifft allerdings nur die Testumgebung.



Die Zertifikate stehen unter [www.chipkarte.at/zertifikate](http://www.chipkarte.at/zertifikate) zur Verfügung.

Im GINS gilt folgende Regel:

- **PROD:** Für den Sessionaufbau im Browser und für das CCS durch den Browser ist ausreichend, wenn das Root Zertifikat PROD eingespielt ist.
  - **VPSWH:** Für den Sessionaufbau im Browser ist ausreichend, wenn das Root Zertifikat Test eingespielt ist; allerdings schlägt der Connectivity Check via CCS durch den Browser fehl. Für einen erfolgreichen Connectivity Check ist auch hier zwingend das Root Zertifikat PROD erforderlich.
- **Ungeduld & langsame GIN-Leitung**  
Ungeduldige Benutzer, die im Browser nicht die Fertigstellung der Tests abwarten

Fortschritt:



Ermittlung Verbindungsstatus Kartenlesegerät abgeschlossen

können, wenn sie zu früh auf den OK Button klicken, eine falsche Anzeige des Ergebnisses erzeugen. In diesem Testfall wird Geduld oft belohnt.

## 4.2 Manuelle Testmöglichkeiten

Für eine funktionierende e-card Anbindung nach dem Hardwaretausch (Abbau der GINA, Kartenlesertausch) sind die Hinweise aus [Kapitel 5: Allgemeine Hinweise zum VP-Netzwerk](#) zu berücksichtigen. Daraus leiten sich im Wesentlichen die folgenden 4 überprüfbaren Punkte ab, die gegeben sein müssen:

- DNS-Auflösung
- Erreichbarkeit des GINS
- direkte Erreichbarkeit des LAN-CCR
- Erreichbarkeit des GINS durch den LAN-CCR

Diese Punkte können manuell folgendermaßen mittels Command Line Befehlen getestet werden.

### 4.2.1 DNS-Auflösung

Mittels nslookup Befehl kann die Namensauflösung für die in [Kapitel 5.2.8: Applikationen und Services](#) angeführten Service-Endpoints geprüft werden.

Anhand des letzten Oktetts der IP-Adresse kann unterschieden werden, über welchen DNS die Namensauflösung erfolgte.

- gerades letztes Oktett (z.B.: 84.38.112.**30**) → Peering Point DNS
- ungerades letztes Oktett (z.B.: 84.38.112.**31**) → öffentlicher DNS

#### 4.2.1.1 Manuelle Prüfung

Request:

nslookup services.ecard.sozialversicherung.at (in Produktion)

nslookup services-a.ecard-test.sozialversicherung.at (in VPSWH-Umgebung)

Erwartete Response:

84.38.112.30 bzw. 84.38.112.31 (in Produktion: PP-DNS bzw. öffentlicher DNS)

84.38.112.28 bzw. 84.38.112.29 (in VPSWH-Umgebung: PP-DNS bzw. öffentlicher DNS)

#### 4.2.2 Erreichbarkeit des GINS

Unter „Erreichbarkeit des GINS“ wird die Kommunikation mit dem e-card System an der GINA „vorbei“, also direkt über den e-card Router, verstanden.

Derzeit (Q3 2021) ist das CCS das einzige Service, das bereits über GINS zu erreichen ist.

Der einfachste Weg ist es, mittels curl einen http GET Request an die /status Ressource des CCS abzusetzen.

##### 4.2.2.1 Manuelle Prüfung CCS

Request:

```
curl -i https://services.ecard.sozialversicherung.at/ccs/1/status (in Produktion)
curl -i https://services-a.ecard-test.sozialversicherung.at/ccs/1/status (in VPSWH)
```

Erwartete Response:

```
HTTP/1.1 200 OK
```

##### 4.2.2.2 Manuelle Prüfung GINS ab dem 1.1.2022

Mit dem 1.1.2022 werden alle e-card Services via GINS erreichbar sein. In der VPSWH-Umgebung ist diese Art der Servicenutzung bereits jetzt möglich.

Eine relativ einfache Testmöglichkeit ist die Abfrage der verfügbaren Kartenleser mittels eines REST-Request an das Card Reader Service (CRS).

Hinweis: Durch den Aufruf der /readers Ressource erhält man die lokalen IP-Adressen der Kartenleser (Parameter „checkIp“), die für den Test der direkten Konnektivität zwischen VP-Software und Kartenleser verwendet werden können.

Request:

```
curl -i https://services.ecard.sozialversicherung.at/crs/1/readers (in Produktion)
curl -i https://services-a.ecard-test.sozialversicherung.at/crs/1/readers (in VPSWH)
```

Beispielresponse:

```
HTTP/1.1 200 OK
Date: Thu, 01 Jul 2021 10:30:43 GMT
Server: Apache
Cache-Control: no-store
Content-Type: application/json;charset=utf-8
Content-Length: 857
Connection: close
Vary: Accept-Encoding
[{"id":",CCR1 (02:0d:87)", "ip":["10.134.240.17"], "checkIp":"10.134.247.62", "type":"LANCCR"}
,{"id":",CCR2 (02:41:55)", "ip":["10.134.240.17"], "checkIp":"10.134.247.61", "type":"LANCCR"}]
```

Die VP-Software kann ab dem 1.1.2022, durch den Wechsel auf den zentralen Servicemanager das GINS nutzen. Wenn der Aufruf von getServices über services.ecard.sozialversicherung.at erfolgreich ist, enthalten die zurückgelieferten Service-URLs keine GINA-IP mehr.

Request (in ASWH):

```
curl --insecure -X POST --data "<soapenv:Envelope
xmlns:soapenv=\"http://schemas.xmlsoap.org/soap/envelope/\"
xmlns:soap=\"http://soap.client.chipkarte.at/\"> <soapenv:Header>
<soapenv:Body><soap:getServices/></soapenv:Body></soapenv:Envelope>" -H "Content-
Type: text/xml;charset=UTF-8" https://services-a.ecard-
test.sozialversicherung.at/servicemanager/1
```

Beispielresponse:

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <getServicesResponse xmlns="http://soap.client.chipkarte.at">
      <return>
        <description>Arzneimittelbewilligungsservice</description>
        <endpointURL>https://services-a.ecard-
test.sozialversicherung.at:443/abs/12</endpointURL>
        <name>abs</name>
        <type>wrapped/literal</type>
        <version>12</version>
      </return>
      <return>
        <description>Attachment Transfer Service</description>
        <endpointURL>https://transfer-a.ecard-
test.sozialversicherung.at:443/ats/1</endpointURL>
        <name>ats</name>
        <type>REST</type>
        <version>1</version>
      </return>
      <return>
        .....
      </return>
    </getServicesResponse>
  </soap:Body>
</soap:Envelope>

```

#### 4.2.3 Direkte Erreichbarkeit des LAN-CCR

Die VP-Software muss die bestehenden LAN-CCR direkt erreichen<sup>20</sup> können.

Mittels eines http GET Requests auf die lokale IP des Kartenlesers kann die Konnektivität geprüft werden.

Ist die lokale IP des Kartenlesers nicht bekannt, kann diese über folgende Methoden erhalten werden:

- Web-Oberfläche  
Mittels Systemstatusinformationen anzeigen → LAN-Kartenleserstatus anzeigen
- CRS  
Aufruf der /readers Ressource und Auswertung des „checkIp“ Response Parameters.

Beispielrequest:

```
curl -i 10.134.247.62
```

Erwartete Response:

```

HTTP/1.1 301 Moved Permanently
Location: https://10.134.247.62/
Content-Length: 0
Date: Fri, 03 Sep 2021 12:39:54 GMT
Server: lighttpd/1.4.55

```

<sup>20</sup> Im Normalfall wird im Zuge der Umstellung der GINO netzwerktechnisch an die gleiche Stelle kommen, an der zuvor der LAN-CCR vorhanden war. Unter dieser Bedingung macht der Test Sinn: ist jetzt der LAN-CCR direkt erreichbar, wird es auch der GINO sein.

#### 4.2.4 Erreichbarkeit des GINS durch den LAN-CCR

Der LAN-CCR führt einen Selbstcheck aus, ob er die folgenden Komponenten via GINS erreicht:

- GINS selbst (mittels CCS)
- SSH
- NTP
- KALVE (Kartenleserverwaltung)
- OCSP (Online Certificate Status Protocol)

Die Ergebnisse des „Selbsttests“ können über die `checkDetails` Ressource des CCS abgefragt werden. Die folgenden Parameter sind dabei verpflichtend anzugeben:

- Kartenleser-ID (`lanccrId`)
- Kartenleser-IP (`lanccrIp`)
- Vertragspartnernummer des VP (`vpnr`)

##### 4.2.4.1 Manuelle Prüfung

Request (in ASWH):

```
curl --insecure -X POST --data "{\"lanccrId\": \"Reader1 (02:0d:87)\",  
\"lanccrIp\": \"10.134.247.62\", \"vpnr\": \"026493\"}" -H "Content-Type: application/json"  
https://services-a.ecard-test.sozialversicherung.at/ccs/1/checkDetails
```

Beispielresponse:

```
{"kalveErreichbar":true,  
"lastConnection":"06.09.2021",  
"lanccrErreichbar":true,  
"ntpsErreichbar":true,  
"sshsErreichbar":true}
```

## 5 Allgemeine Hinweise zum VP-Netzwerk

### 5.1 DNS Auflösung

Um die im Dokument angeführten QoS Hostnamen und auch weitere, für den GINO notwendige Hosts (NTP, Kartenleserverwaltung KALVE), auflösen zu können, stehen folgende DNS-Server zur Verfügung:

84.38.113.161  
84.38.113.162

Für Produktion und Testsystem gelten die gleichen DNS-Server.

Es wird nicht mehr empfohlen (wie es bisher üblich war), die GINA (IP) als DNS zu verwenden, wenn eine statische IP-Konfiguration oder ein eigener DHCP-Server genutzt wird!

Im Zuge des Rollouts wird die GINA durch den Providertechniker abgebaut und steht daher nicht mehr als DNS-Server zur Verfügung. Zeitgleich ändert der Providertechniker die (optionale) DHCP-Konfiguration am e-card Router auf die neuen DNS-Server.

Für GINOs ist zu beachten, dass für eine korrekte Funktionalität auch auf diesen Geräten die DNS Auflösung funktionieren muss. Im Standardfall haben diese dann direkt den DNS 84.38.113.161 bzw. 84.38.113.162 eingetragen oder müssen entsprechend konfiguriert werden.

Aktuell: für statisch konfigurierte LAN-CCRs, die keinen DNS eingetragen haben, wird der DNS **84.38.113.161** einmal pro Woche (jeweils an einem anderen Wochentag) per Script eingetragen. In allen anderen Fällen (eigener DNS) muss ggf. eine manuelle Anpassung erfolgen.

#### 5.1.1 Verwendung eines internen DNS im VP-Netzwerk

Bei Verwendung eines internen DNS im VP-Netzwerk soll ein Forward von

[\\*.ecard.sozialversicherung.at](http://*.ecard.sozialversicherung.at) und  
[\\*.ecard-test.sozialversicherung.at](http://*.ecard-test.sozialversicherung.at) und  
[\\*.pki.sozialversicherung.at](http://*.pki.sozialversicherung.at)

auf oben genannte Server eingerichtet werden; der Rest wird auf den Default-DNS weitergeleitet.

#### 5.1.2 Verwendung eines öffentlichen DNS

Auch wenn die Verwendung des Peering Point / e-card DNS die korrekte Lösung darstellt, kann dies für relativ einfache VP-Netzwerke mit GIN Anschluss und einem zweiten, zusätzlichen Internet Anschluss („Business“-Internet) eine Herausforderung darstellen.

Aus diesem Grund werden alle für die Verwendung der e-card Services notwendigen Hostnamen auch über öffentliche DNS-Server aufgelöst.

**Dabei gelten aber folgende, wichtige Einschränkungen:**

- **Eingeschränkte Funktionalität**  
Durch die Verwendung eines öffentlichen DNS für die Namensauflösung ist die Funktionalität des e-card Systems beim VP auch von der Verfügbarkeit des zusätzlichen Internet-Anschlusses abhängig.  
Fällt das „Business“-Internet aus oder die dort verwendete DNS-Auflösung, so ist für den Client auch das grundsätzlich noch immer funktionierende e-card System nicht mehr erreichbar, da die notwendige Namensauflösung fehlschlägt.

- **Kein Support/keine Abrechnungsgarantie im Fehlerfall**  
Bei Ausfall des „Business“-Internets und wenn der v das e-card System dadurch nicht mehr verwenden kann, kann kein Support seitens Service-Line geleistet werden und auch keine Abrechnungsgarantie erfolgen.

## 5.2 DNS und Routing im VP-Netzwerk – Zusammenfassung

### 5.2.1 Ausgangslage

#### 5.2.1.1 GIN Anschluss (standardmäßig ein GIN Anschluss)

Vorgaben für Netzwerk-Konfigurationen:

- Default Gateway am GIN Router
- DHCP am GIN Router
- Eintragen von Routen nicht notwendig
- GINOs werden voraussichtlich in Zukunft statisch konfiguriert (um die Wunsch-IP dauerhaft für die VP-Software und Browser festzulegen)
- **Änderungen oder Eintragungen von Routen am e-card GIN-Router sind nicht erforderlich.**

#### 5.2.1.2 GIN Anschluss und ein weiterer Internet Router im Netz

- **kein Netzwerk-Support durch SVC**
- Default Gateway (ist meist der Internet-Router - je nach Anforderungen)
- Eintragen von Routen Richtung GIN **unbedingt** erforderlich (siehe [Routing Hinweise](#))
- DHCP nicht unbedingt erforderlich – muss, wenn vorhanden, eindeutig auf einem Router definiert werden  
(Achtung: Vorgaben bez. zugelassener **interner Netze** beachten, wenn der DHCP-Server durch den Internet-Router zur Verfügung gestellt wird)
- GINOs müssen statisch konfiguriert werden
- DNS Hinweis beachten (siehe [DNS Hinweis](#))
- **Änderungen oder Eintragungen von Routen am e-card GIN-Router sind nicht erforderlich.**

### 5.2.2 Interne VP-Netze

Unterstützte Netze:

- 192.168.0.0/16
- für Arzt-Ordinationen: 10.0.0.0 bis 10.127.255.255
- für Apotheken: 10.0.0.0 bis 10.127.255.255

Netze die im VP-LAN nicht verwendet werden dürfen:

- Arzt-Ordination: 10.128.0.0 bis 10.255.255.255
- Apotheke: 10.128.0.0 bis 10.255.255.255
- 172.16.0.0 bis 172.31.255.255 (e-card Services)

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 am 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.

**Wichtig: Achten Sie auf den „Full-NAT“ IP-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**.)

Details dazu, siehe GIN-Netzwerkdokument Kapitel 3.4 „Netz für das LAN des VP (alias Ordinations-LAN)“.

### 5.2.3 DNS Hinweise

Siehe Kapitel 5.1 [DNS Auflösung](#)

### 5.2.4 Routing Hinweise

Folgende Netze müssen zum GIN geroutet werden:

- **84.38.112.0/20**  
→ zum e-card Router
- **172.16.0.0/12** (172.16.0.0 bis 172.31.255.255)  
→ zum e-card Router (für Dienste am PP, wie zum Beispiel MWD-Anbieter)

...inklusive folgender **HEALIX Netze**:

- 79.174.96.0/19 (HEALIX MWD)
- 193.46.140.0/24 (HEALIX MWD)
- 193.46.141.0/24 (HEALIX MWD)
- 193.46.142.0/24 (HEALIX MWD)

*Zweck: im HEALIX können auch MWD Services durch Krankenanstalten angeboten werden.*

... und folgende private Netze:

- 10.128.0.0/9 (gilt auch<sup>21</sup> für APO)

*Zweck: wenn jemand keine weitere Infrastruktur vor Ort hat und einen Internet-Router zusätzlich im VP-LAN betreibt, ist das die langlebigste Konfiguration (weil diese RFC 1918 Netze nicht im Internet existieren).*

Hinweis: Das erspart Konfigurationsanpassungen in den nächsten Jahren.

Auch private Netze (RFC 1918, ausgenommen 192.168.0.0/16) sollen ins GIN geroutet werden, wenn ein anderer Router/Modem als der e-card Router als Default-Gateway genutzt wird.

(Hintergrund: Private Netze existieren im Internet nicht, könnten aber in Zukunft im GIN genutzt werden. Dies erspart spätere Anpassungen. Ausnahme: Es werden Teile der privaten Netze im VP-Netzwerk verwendet.)

Für Details zum Routing siehe GIN-Netzwerkdokument Kapitel: "6 Routing im Netzwerk des VP".

---

<sup>21</sup> Siehe Erläuterungen in Kapitel [5.2.2 Interne VP Netze](#)  
CCS Kurzanleitung

### 5.2.5 Secure-NTP (für GINO)

Für den GINO muss ein NTP erreichbar sein (im Fall der statischen Konfiguration muss dieser manuell konfiguriert werden).

NTP für produktive GINOs:

- [ntp1.ecard.sozialversicherung.at](http://ntp1.ecard.sozialversicherung.at) = 84.38.113.163 TCP+UDP 123
- [ntp2.ecard.sozialversicherung.at](http://ntp2.ecard.sozialversicherung.at) = 84.38.113.164 TCP+UDP 123
- [ntp3.ecard.sozialversicherung.at](http://ntp3.ecard.sozialversicherung.at) = 84.38.113.165 TCP+UDP 123
- [ntp4.ecard.sozialversicherung.at](http://ntp4.ecard.sozialversicherung.at) = 84.38.113.166 TCP+UDP 123

NTP für SWH GINOs:

- [ntps1.ecard.sozialversicherung.at](http://ntps1.ecard.sozialversicherung.at) = 84.38.113.167 TCP+UDP 123
- [ntps2.ecard.sozialversicherung.at](http://ntps2.ecard.sozialversicherung.at) = 84.38.113.168 TCP+UDP 123
- [ntps3.ecard.sozialversicherung.at](http://ntps3.ecard.sozialversicherung.at) = 84.38.113.169 TCP+UDP 123
- [ntps4.ecard.sozialversicherung.at](http://ntps4.ecard.sozialversicherung.at) = 84.38.113.170 TCP+UDP 123

GINOs aus der Testumgebung müssen ntps\* Server erreichen; produktive GINOs müssen ntp\* Server erreichen!

### 5.2.6 Kartenleserverwaltung

Kartenleser (KALVE) + GINO Fernwartung (SSH):

- [kalve.ecard.sozialversicherung.at](http://kalve.ecard.sozialversicherung.at)
  - 84.38.112.30 / TCP 451 bis 454 + 10022 und 20022
  - 84.38.112.31 / TCP 451 bis 454 + 10022 und 20022
- [kalve-a.ecard-test.sozialversicherung.at](http://kalve-a.ecard-test.sozialversicherung.at)
  - 84.38.112.28 / TCP 451 bis 454 + 10022 und 20022
  - 84.38.112.29 / TCP 451 bis 454 + 10022 und 20022

### 5.2.7 OCSP

- [ocsp.pki.sozialversicherung.at](http://ocsp.pki.sozialversicherung.at)
  - 84.38.112.14 / Port 80
  - 84.38.112.15 / Port 80
- [ocsp-test.pki.sozialversicherung.at](http://ocsp-test.pki.sozialversicherung.at)
  - 84.38.112.12 / Port 80
  - 84.38.112.13 / Port 80

### 5.2.8 Applikationen und Services

Auch hier gilt die Trennung von Produktion und Testsystem.

#### Applikationen und Services (GINS-PROD)

QoS	Hostname	IP	Port
hoch	<a href="http://services.ecard.sozialversicherung.at">services.ecard.sozialversicherung.at</a>	84.38.112.30, 84.38.112.31	443 und 80
mittel	<a href="http://elga.ecard.sozialversicherung.at">elga.ecard.sozialversicherung.at</a>	84.38.112.60, 84.38.112.61	443 und 80
niedrig	<a href="http://transfer.ecard.sozialversicherung.at">transfer.ecard.sozialversicherung.at</a>	84.38.112.90, 84.38.112.91	443 und 80



### Services (GINS-Testsystem)

QoS	Hostname	IP	Port
hoch	<a href="http://services-a.ecard-test.sozialversicherung.at">services-a.ecard-test.sozialversicherung.at</a>	84.38.112.28, 84.38.112.29	443 und 80
mittel	<a href="http://elga-a.ecard-test.sozialversicherung.at">elga-a.ecard-test.sozialversicherung.at</a>	84.38.112.58, 84.38.112.59	443 und 80
niedrig	<a href="http://transfer-a.ecard-test.sozialversicherung.at">transfer-a.ecard-test.sozialversicherung.at</a>	84.38.112.88, 84.38.112.89	443 und 80

Die IP-Adressen mit gerader Zahl im letzten Oktett werden über den Peering Point / e-card DNS aufgelöst; jene mit ungeradem letzten Oktett über den öffentlichen DNS.

#### 5.2.9 GINA-IP vs. Client-IP / Anschluss-IP – MyIP Auskunftsservice

Mit der Umstellung der Kommunikation auf GINS, fällt die GINA-IP als Identifikationsmerkmal des Anschlusses im Support- oder Incident-Fall weg. Grundsätzliches Identifikationsmerkmal ist und bleibt die VPNR (Vertragspartnernummer); dennoch stellt die Client- bzw. Anschluss-IP eine wichtige Information dar.

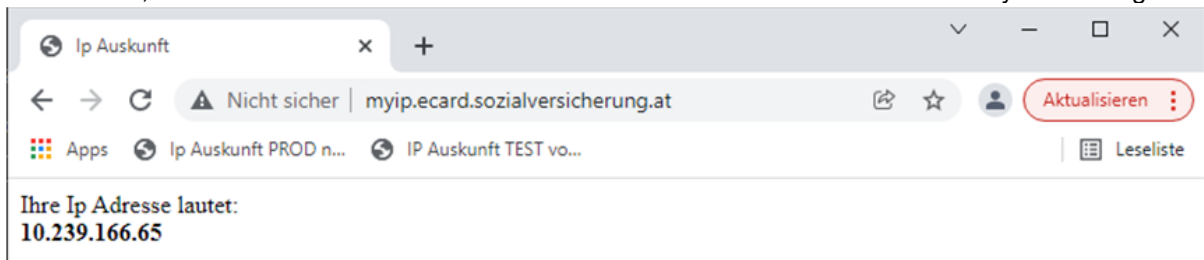
#### MyIP Auskunftsservice

Durch den Aufruf von

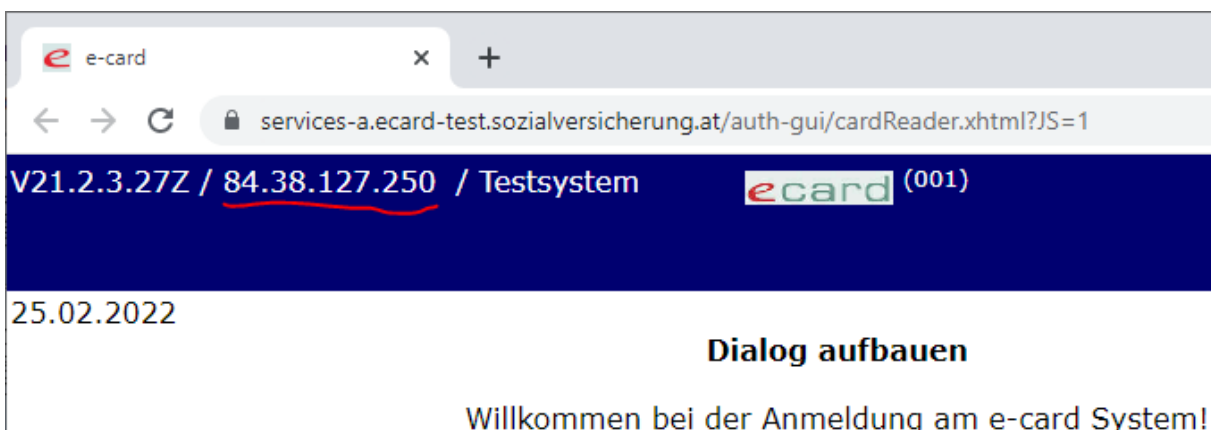
<http://myip.ecard.sozialversicherung.at> 84.38.113.190 (PP DNS) bzw. 84.38.113.191 (Internet DNS)

bzw. <http://myip.ecard-test.sozialversicherung.at>

erfährt man, mit welcher Client- bzw. Anschluss-IP die Kommunikation zum e-card System erfolgt.



Alternativ findet sich die Client-/Anschluss-IP auch in der Maske der e-card Web-Oberfläche, sofern diese über <https://services.ecard.sozialversicherung.at> aufgerufen wurde. Die Information findet sich an der Stelle, an der zuvor die GINA-IP zu finden war.



### 5.3 Nating von LAN-CCRs und CCS

Für den Fall, dass im VP-LAN die IP-Adresse von LAN-CCRs mittels NAT (Network Address Translation) übersetzt wird, schlägt die `/checkDetails` Abfrage des CCS für diesen Kartenleser fehl.<sup>22</sup> Die Funktionalität im Zuge der GINS-Umstellung ist davon jedoch nicht beeinträchtigt. Auch der Einsatz eines GINO in Verbindung mit NAT stellt kein Problem dar.

#### Hintergrund:

Die GINA kommuniziert über den e-card Router direkt mit den Kartenlesern (LAN-CCRs). Dabei „sieht“ sie die Kartenleser mit der IP, mit der die Pakete des LAN-CCRs am e-card Router ankommen; also im Falle von Nating mit einer übersetzten IP-Adresse. Diese Adressen werden von der GINA an das CRS gemeldet, welches via der Ressource `/readers` oder `/readersUrl` dazu verwendet werden kann, die Liste der Kartenleser und deren „checkIp“ zu bekommen.

Wenn der LAN-CCR seinen „Selbsttest“ durchführt, dann kommuniziert er mit dem CCS und teilt diesem seine derzeitige, lokale IP-Adresse mit. Eine spätere Anfrage eines Client-PCs via e-card Web-Oberfläche oder VP-SW (Ressource `/checkDetails` des CCS), die als Parameter die genatete „checkIp“ enthält, wird keine Einträge finden, die mit der tatsächlichen IP des Kartenlesers gespeichert wurden, und wird daher ein leeres Ergebnis liefern.

#### Beispiel:

Die Client-PCs und der Server einer Ordination sind im NW-Segment 10.160.1.0/24. (Hinweis: dieser NW-Bereich ist für die direkte Kommunikation mit dem e-card System nicht zugelassen.) Der e-card Router hat die IP 192.168.1.254 und das Subnetz eine NW-Maske von 255.255.255.0 also 192.168.1.0/24.

Der LAN-CCR hat die lokale IP 10.160.1.82. Mit dieser macht er seinen CCS-„Selbsttest“ und die Ergebnisse werden zur IP 10.160.1.82 gespeichert. In das NW-Segment des e-card Routers erfolgt ein NAT auf 192.168.1.82. Unter dieser IP „findet“ die GINA den LAN-CCR und das ist auch die „checkIp“, die vom CRS zurückgeliefert wird. Fragt nun ein Client-PC (dessen IP in diesem Beispiel ebenfalls genatet werden muss) nun `/checkDetails` mit dem Parameter 192.168.1.82 für die IP des Kartenlesers an, ist die Antwort leer. Das CCS würde einen Fehler liefern, obwohl die Funktionalität gegeben ist.

#### Lösung:

Das Ergebnis der `/checkDetails` Ressource von genateten Kartenlesern muss ignoriert werden bzw. muss für `/checkDetails` die lokale IP-Adresse des Kartenlesers verwendet werden.

#### 5.3.1 NAT und GINO

Bei der Verwendung von GINOs kann das oben beschriebene Problem nicht auftreten. Der GINO kommuniziert selbst direkt mit der KALVE (Kartenleserverwaltung) und teilt dieser seine lokale IP-Adresse mit. Diese wird dann vom CRS zurückgeliefert (`/readers` oder `/readersUrl`). Nachdem das e-card System nie von sich aus eine Verbindung zum GINO aufbaut, sondern dieser immer eine Kommunikation initiieren muss, stellt ein NAT auch in Bezug auf Firmware-Updates oder sonstiges kein Problem dar.

---

<sup>22</sup> Schlägt fehl, wenn bei `/checkDetails` die NAT IP-Adresse mitgeschickt wird. Wenn die lokale IP-Adresse geschickt wird, sollte ein Ergebnis retour kommen, wenn sich der LAN-CCR erfolgreich gemeldet hat.  
CCS Kurzanleitung