Network evidence report

Example Health · 2.4.0 (187) · session 1

Session

Project	Example Health
App bundle identifier	com.example.health
Session	1
Kind	audit
Release	2.4.0 (187)
Started	2027-01-15T02:02:31.759Z
Ended	2027-01-15T07:29:20.683Z
Device	iPhone18,3
iOS	26.5
Recorded with TunnelVision	1.0.0 (1)
Exported with TunnelVision	1.0.0 (1)
Exported	2027-01-15T09:00:00.000Z
TLS inspection	on
Local CA trusted	yes
Notes	Fresh install, onboarding to first sync.

Inspection was on and the local CA was trusted: whether a connection accepted or refused the local CA's certificate can be read from this session.

Markers

Instant (UTC)	Marker	Label
2027-01-15T03:24:13.990Z	consentGiven	
2027-01-15T04:45:56.221Z	loggedIn	
2027-01-15T06:07:38.452Z	custom	First sync finished

Allowlist

Pattern	Note
api.example-health.com	Backend
*.cdn.example-health.com	Static assets
telemetry.example-crash.io	Crash reporting

How to read this report

> The tunnel sees packets, not processes: every flow that carried traffic while the session was open is listed, whichever app sent it. Attribution to the audited app is procedural: a controlled device, compared against a baseline session recorded without the app.

> A verdict states what the recorded traffic showed, within the toolCoverage of its requirement. It is not a test result: the results of TR-03161 are the assessor's to give. No verdict states that a requirement is met, and a requirement with no applicable observation is not assessed by this tool.

> Connection metadata, what it shows against a requirement catalogue, and a capture of the session's packets as they crossed the tunnel. Decrypted content is not part of this bundle.

> Connection metadata only: no payloads. Certificate fields are what the server presented; nothing was validated. A TLS answer with source upstreamConnection is what the server negotiated with the tunnel's own connection, not with the app. A key that is absent is a reading that was not made.

Requirement catalogue

Catalogue	tr-03161-1_3.0
Document	BSI TR-03161-1
Title	Anforderungen an Anwendungen im Gesundheitswesen – Teil 1: Mobile Anwendungen
Version	3.0 (2024-03-25)
SHA-256 of the PDF it was checked against	f8837fbee1710ad3555bbe333f4a50e83c0c66b24724ab3be5cc634a80beb001

Minimum TLS version

Lowest version accepted	TLS 1.2
Document	BSI TR-02102-2
Title	Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2: Verwendung von Transport Layer Security (TLS)
Version	2026-01 (2026-01-27)
SHA-256 of the PDF it was checked against	eed80d1a38ec0d7d8908765c3a09ea6f17a7ca729bef95b0d358d5d129af3f1f

Requirements

Requirement	Verdict
O.Purp_3	Contradicted by observations of this session.
O.Purp_8	Contradicted by observations of this session.
O.Ntwk_1	Contradicted by observations of this session.
O.Ntwk_2	Contradicted by observations of this session.
O.Ntwk_3	Not assessed by this tool.
O.Ntwk_4	Contradicted by observations of this session.
O.Ntwk_5	Not assessed by this tool.
O.Ntwk_6	Not assessed by this tool.
O.Ntwk_7	Not assessed by this tool.
O.Ntwk_8	Not assessed by this tool.

O.Purp_3 — Einholung einer Einwilligungserklärung des Nutzers.

Test aspect	1 Anwendungszweck
Test depth	CHECK
Verdict	Contradicted by observations of this session.
Tool coverage (toolCoverage)	Compares when each connection opened with the consent markers placed during the session. A connection opened before consent is network activity, not proof that personal data was processed, and the tunnel cannot tell which app opened it.
Findings against it	F2
Check behind it	Activity before consent (consent)
Connections opened after every consent marker	57
Connections not assessed	0
Connections the check does not apply to	0

O.Purp_8 — Weitergabe von sensiblen Daten nur für den primären oder rechtmäßigen Zweck.

Test aspect	1 Anwendungszweck
Test depth	CHECK
Verdict	Contradicted by observations of this session.
Tool coverage (toolCoverage)	Compares the host of each connection with the project's allowlist, and lists the connections that had no name to compare. A host outside the allowlist is a connection to an unlisted party; whether sensitive data was sent to it, and whether the user agreed, is not observed.
Findings against it	F1, F3, F4, F5, F6, F8, F9, F10, F12, F13, F15, F17, F18, F19, F20, F21, F22, F23, F24, F26, F27, F28, F29, F30, F32, F33, F35, F36, F38, F39, F40, F41, F42, F44, F45, F46, F47, F48, F49, F50, F51, F52, F54, F56, F57, F58, F59, F60, F61, F62, F63, F64
Check behind it	Destination against the allowlist (host)
Connections to a host the allowlist covers	0
Connections not assessed	0
Connections the check does not apply to	0

O.Ntwk_1 — Netzwerkkommunikation durchgängig mit gegenseitiger Authentisierung verschlüsselt.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Contradicted by observations of this session.
Tool coverage (toolCoverage)	Raised only by an HTTP request that was seen in the clear. Mutual authentication is not observed: a connection seen to be encrypted says nothing about a client certificate.
Findings against it	F7
Check behind it	Encryption (encryption)

Connections seen to be encrypted	50
Connections not assessed	1
Connections the check does not apply to	3

O.Ntwk_2 — Konfiguration der verschlüsselten Verbindung gemäß aktuellem Stand der Technik.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Contradicted by observations of this session.
Tool coverage (toolCoverage)	Compares the negotiated TLS version with the lowest one TR-02102-2 recommends. Cipher suites, key agreement groups and signature algorithms are not compared with its tables.
Findings against it	F11
Check behind it	TLS version (tlsVersion)
Connections at or above the minimum TLS version	49
Connections not assessed	0
Connections the check does not apply to	13

O.Ntwk_3 — Sichere Kommunikationskanäle nur mit Betriebssystem-Funktionen oder sicherheitsüberprüfter Drittsoftware.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Not assessed by this tool.

O.Ntwk_4 — Unterstützung von Zertifikats-Pinning.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Contradicted by observations of this session.
Tool coverage (toolCoverage)	Reads, per host, whether connections accepted or refused a certificate issued by the local inspection CA, and only in a session recorded with inspection on and that CA trusted. A refusal does not tell pinning apart from refusing every user-installed root, it may predate the session, and nothing is bypassed to find out more.
Findings against it	F14, F25, F31, F34, F37, F43, F53, F55, F65
Findings in its support	F16
Check behind it	Certificate pinning (pinning)
Connections not assessed	39
Connections the check does not apply to	13

O.Ntwk_5 — Validierung des Server-Zertifikats des Hintergrundsystems.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Not assessed by this tool.

O.Ntwk_6 — Validierung der Integrität und Authentizität der Antworten des Hintergrundsystems.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Not assessed by this tool.

O.Ntwk_7 — Verwendung plattformspezifischer Optionen.

Test aspect	9 Netzwerkkommunikation
Test depth	EXAMINE
Verdict	Not assessed by this tool.

O.Ntwk_8 — Vorhaltung von vollständigen Log-Dateien für alle aufgebauten Verbindungen.

Test aspect	9 Netzwerkkommunikation
Test depth	CHECK
Verdict	Not assessed by this tool.

Findings

unnamedFlow

> A connection has no name to compare with the allowlist: no ClientHello was read from it and no DNS reply seen by the tunnel named its address.

Finding	Connections	Flows in flows.json
F1	4	7, 10, 11, 12

activityBeforeConsent

> A connection was opened before every consent marker of the session.

Finding	Connections	Flows in flows.json
F2	6	7, 38, 18, 46, 9, 55

hostNotInAllowlist

> A connection went to a host that the project's allowlist does not cover.

Finding	Stated about	Connections	Flows in flows.json
F3	media37.example.com	1	38
F4	media17.example.com	2	18, 58
F5	log5.example.com	1	46
F6	very-long-subdomain-name-that-will-not-fit.cdn.assets.example.com	1	9
F8	sync14.example.com	1	55
F9	static1.example.com	1	42
F12	reset.example.org	1	13

Finding	Stated about	Connections	Flows in flows.json
F13	stream.example.com	1	4
F15	pinned.example.net	1	5
F17	log25.example.com	1	26
F18	mail29.example.com	1	30
F19	log35.example.com	1	36
F20	img32.example.com	1	33
F21	sync4.example.com	1	45
F22	img12.example.com	1	53
F23	auth36.example.com	1	37
F24	edge28.example.com	1	29
F26	img22.example.com	2	63, 23
F27	cdn30.example.com	1	31
F28	uncaptured.example.org	1	14
F29	img2.example.com	1	43
F30	api23.example.com	1	24
F32	sync24.example.com	1	25
F33	edge18.example.com	2	19, 59
F35	downloads.example.com	1	15
F36	api13.example.com	1	54
F38	static11.example.com	1	52
F39	www.example.com	1	2
F40	api33.example.com	1	34
F41	mail19.example.com	2	20, 60
F42	edge38.example.com	1	39
F44	auth16.example.com	2	57, 17
F45	log15.example.com	2	16, 56
F46	cdn0.example.com	1	41
F47	auth6.example.com	1	47
F48	cdn20.example.com	2	21, 61
F49	auth26.example.com	1	27
F50	quic.example.com	1	6
F51	mail9.example.com	1	50
F52	api.example.com	1	3
F54	edge8.example.com	1	49
F56	sync34.example.com	1	35
F57	mail39.example.com	1	40
F58	cdn10.example.com	1	51

Finding	Stated about	Connections	Flows in flows.json
F59	plain.example.org	1	1
F60	static31.example.com	1	32
F61	media7.example.com	1	48
F62	static21.example.com	2	22, 62
F63	media27.example.com	1	28
F64	api3.example.com	1	44

cleartextTraffic

> An HTTP request was observed in the clear.

Finding	Connections	Flows in flows.json
F7	9	55, 30, 25, 20, 60, 50, 35, 40, 1

unnamedFlow

> A connection has no name to compare with the allowlist: its ClientHello announced none.

Finding	Connections	Flows in flows.json
F10	1	8

weakTLSVersion

> A connection negotiated a TLS version below TLS 1.2.

Finding	Stated about	Connections	Flows in flows.json
F11	TLS 1.0, serverHello	1	13

pinningAbsent

> A connection to this host accepted a certificate issued by the local CA: for this host, a user-installed root is trusted.

Finding	Stated about	Connections	Flows in flows.json
F14	stream.example.com	1	4
F25	edge28.example.com	1	29
F31	api23.example.com	1	24
F34	edge18.example.com	2	19, 59
F37	api13.example.com	1	54
F43	edge38.example.com	1	39
F53	api.example.com	1	3
F55	edge8.example.com	1	49
F65	api3.example.com	1	44

pinningObserved

> A connection to this host refused the local CA's certificate. The statement is about the host: after a refusal the tunnel does not try that host again, so the refusal may predate this session.

Finding	Stated about	Connections	Flows in flows.json
F16	pinned.example.net	1	5

How far each check got

Each check sorts every connection of the session into one of four groups: it is behind a finding, it was looked at with nothing to report, it could not be assessed (with the reason), or the check does not apply to it. A requirement names the check behind it.

Encryption (encryption)

Connections behind a finding	9
Connections seen to be encrypted	50
Connections not assessed	1
Connections the check does not apply to	3

Why it could not be assessed	Connections
A UDP connection with no recognised QUIC header. Its datagrams are not read beyond that; DNS on port 53 is counted here.	1

TLS version (tlsVersion)

Connections behind a finding	1
Connections at or above the minimum TLS version	49
Connections not assessed	0
Connections the check does not apply to	13

Destination against the allowlist (host)

Connections behind a finding	63
Connections to a host the allowlist covers	0
Connections not assessed	0
Connections the check does not apply to	0

Certificate pinning (pinning)

Connections behind a finding	11
Connections not assessed	39
Connections the check does not apply to	13

Both outcomes of this check are findings: a connection that accepted the local CA's certificate and one that refused it are each listed under Findings, per host.

Why it could not be assessed	Connections
The connection shows TLS over TCP and carries no inspection outcome: inspection was not attempted on it, or its result is not known.	34

Why it could not be assessed	Connections
The connection is QUIC. Inspection only terminates TLS over TCP.	5

Activity before consent (consent)

Connections behind a finding	6
Connections opened after every consent marker	57
Connections not assessed	0
Connections the check does not apply to	0

TLS and QUIC readings

> One row per host and reading, in the order each was first seen. The last column names where the reading comes from, as flows.json does: serverHello is the server's answer to the app's own ClientHello; upstreamConnection is what the server negotiated with the tunnel's own connection on an inspected connection, not with the app; a QUIC version read from the client is the one it proposed. Nothing about a certificate was validated.

Host	Name from	Reading	Read from	Connections
media37.example.com	sni	TLS 1.3	serverHello	1
media17.example.com	sni	TLS 1.3	serverHello	2
log5.example.com	sni	TLS 1.3	serverHello	1
very-long-subdomain-name-that-will-not-fit.cdn.assets.example.com	sni	TLS 1.3	serverHello	1
static1.example.com	sni	TLS 1.3	serverHello	1
(no name)		TLS 1.3	serverHello	1
reset.example.org	sni	TLS 1.0	serverHello	1
stream.example.com	sni	TLS 1.3	upstreamConnection	1
pinned.example.net	sni	TLS 1.3	upstreamConnection	1
log25.example.com	sni	TLS 1.3	serverHello	1
log35.example.com	sni	TLS 1.3	serverHello	1
img32.example.com	sni	TLS 1.3	serverHello	1
sync4.example.com	sni	QUIC 0x00000001	quic, read from the server	1
img12.example.com	sni	TLS 1.3	serverHello	1
auth36.example.com	sni	TLS 1.3	serverHello	1
edge28.example.com	sni	TLS 1.3	upstreamConnection	1
img22.example.com	sni	TLS 1.3	serverHello	1
cdn30.example.com	sni	TLS 1.3	serverHello	1
uncaptured.example.org	sni	TLS 1.3	serverHello	1
img22.example.com	sni	QUIC 0x00000001	quic, read from the server	1
img2.example.com	sni	TLS 1.3	serverHello	1
api23.example.com	sni	TLS 1.3	upstreamConnection	1

Host	Name from	Reading	Read from	Connections
edge18.example.com	sni	TLS 1.3	upstreamConnection	2
downloads.example.com	sni	TLS 1.3	serverHello	1
api13.example.com	sni	TLS 1.3	upstreamConnection	1
static11.example.com	sni	TLS 1.3	serverHello	1
www.example.com	sni	TLS 1.2	serverHello	1
api33.example.com	sni	QUIC 0x00000001	quic, read from the server	1
edge38.example.com	sni	TLS 1.3	upstreamConnection	1
auth16.example.com	sni	TLS 1.3	serverHello	2
log15.example.com	sni	TLS 1.3	serverHello	1
cdn0.example.com	sni	TLS 1.3	serverHello	1
auth6.example.com	sni	TLS 1.3	serverHello	1
cdn20.example.com	sni	TLS 1.3	serverHello	2
auth26.example.com	sni	TLS 1.3	serverHello	1
quic.example.com	dns	QUIC 0x00000001	quic, read from the server	1
api.example.com	sni	TLS 1.3	upstreamConnection	1
log15.example.com	sni	QUIC 0x00000001	quic, read from the server	1
edge8.example.com	sni	TLS 1.3	upstreamConnection	1
cdn10.example.com	sni	TLS 1.3	serverHello	1
static31.example.com	sni	TLS 1.3	serverHello	1
media7.example.com	sni	TLS 1.3	serverHello	1
static21.example.com	sni	TLS 1.3	serverHello	2
media27.example.com	sni	TLS 1.3	serverHello	1
api3.example.com	sni	TLS 1.3	upstreamConnection	1

Connections with a reading	50
Connections with no TLS or QUIC reading	13

Capture

capture.pcapng does not hold every packet the session recorded. A connection with few packets in it is not a connection with little traffic: the counts below, and capture.json for each connection, say what is not there.

Packets recorded	4895
Packets in capture.pcapng	4842
Never written to a capture file (notCaptured)	53

> The packets of this session's flows whose bytes were still on the device when the bundle was exported, as raw IP datagrams in the order they were captured. Each packet is written as it crossed the tunnel: what was encrypted on the wire is encrypted here, and what was sent in the clear is readable here. A packet counted under withoutBytes is in the history and not in the capture: notCaptured was never written to a capture file, captureFileMissing was in a capture file that is no

> longer on the device, and recordUnreadable could not be read back from its file. A flow belongs to the session when it carried traffic while the session was open, so its packets from before or after are included too, and counted under writtenOutsideSession.

> Every packet carries a comment, "flow=<id>" or "flow=<id> findings=<id>,<id>": the flow it belongs to, as listed in flows.json, and the findings of findings.json which that flow is evidence of. It also carries its direction as seen from the device. In Wireshark, frame.comment matches "flow=12(|$)" shows one flow, and frame.comment matches "F3(,|$)" the packets behind one finding.