Secure Call Flows

Section	Description
Feature Area	Architect / Flows
Flow Type	Secure Call Flow
Navigation	`Admin → Architect → Flows → Secure Call`
Primary Function	Temporarily mask audio and prevent recording/agent access to sensitive customer data (PCI payments, PII collection)
Compliance	**PCI DSS compliant**

Secure call flows protect sensitive customer data by masking audio paths and preventing system recording during specific portions of an interaction. The most common use case is collecting credit card or bank account information for payment processing without exposing that data to agents or recording systems.

Study Notes

Topic	Explanation
Secure Flow	A flow type in Architect that masks audio and data captured during an interaction to meet PCI/PII compliance requirements
Secure IVR	Bundles multiple tools — secure flows, secure variables, and secure actions — into a complete PCI-safe data collection approach
Secure Action	Any action in Architect marked as "secure" — triggers the flow to operate in secure mode
Secure Variable	A variable whose content is flagged as secure — also triggers secure mode when consumed
Key Icon	Visual indicator in Architect showing that an action or action beneath it is either secure or consuming secure data
PCI DSS	Payment Card Industry Data Security Standard — secure call flows help organizations comply with this standard for phone-based payments

Topic	Explanation
Protocol Capture risk	Enabling trunk diagnostics/protocol capture logs **all data**, including data entered in secure flows — sensitive data is not encrypted. Avoid enabling when using secure flows
PCI DSS setting	If enabled in org settings, Genesys Cloud **automatically disables** Media Capture and Protocol Capture settings

Two Secure Flow Scenarios

Scenario	Description
Agent-referred secure session	Agent is on an active call with the customer → agent initiates the transfer to a secure flow → flow collects sensitive data → flow returns caller to the agent via **Return to Agent** action
IVR-only secure session	No live agent involved — caller interacts entirely with the automated flow — sensitive data collected and processed — flow ends with **Disconnect** action

Key Actions in Secure Flows

Action	Purpose
Transfer to Secure Flow	Used in an Inbound, Outbound, or In-Queue flow to transfer the caller into a secure flow
Return to Agent	Terminating action in a secure flow — reconnects caller to the agent after the secure session ends; passes stored variable values (e.g., confirmation number) back to agent's script
Disconnect	Terminating action for IVR-only secure sessions with no agent
Extract Secure Data	Retrieves secure variable values within a secure flow
Call Secure Data	Used to pass secure data between flow components

> The **Transfer to Secure Flow** action is available in Inbound, Outbound, and In-Queue flows. For transfer actions **within** a secure flow: Genesys Cloud uses **blind transfers** (not consult). The defined failure path is overridden and the call is disconnected if the transfer fails.

Return to Agent Action — Key Details

Attribute	Detail
Type	Terminating action — ends the secure flow
Where used	Secure flows (agent-referred scenario)
What it does	Reconnects caller to the original agent; sends stored variable values to agent's script
If agent left before caller returns	Call is **disconnected**
Cannot transfer to new destination	Return to Agent does not support transferring to a different agent or number
Monitoring restriction	If a supervisor is actively monitoring the interaction, the agent **cannot** initiate the Transfer to Secure Flow; monitoring must be ended first

Analytics Impact

Secure flows affect the following agent metrics:

Metric Affected	Description
Time in IVR	Time spent in the secure flow counts against IVR time
Average Time in IVR	Affected by secure flow duration
Agent Handle Time	Impacted because the agent is technically handling the interaction during the secure session
Average Agent Handle Time	Affected
Agent Talk Time	Affected

Bot Integration with Secure Flows

If a bot session is initiated from a secure call flow, the bot **inherits the secure characteristics** of the secure call flow. This prevents logging and recording of data at the bot level, maintaining

PCI/PII compliance.

> **Note:** Dialog Engine Bot Flows are **PCI DSS compliant** and can be used in secure call flows. Digital Bot Flows are **not PCI DSS compliant** and must **not** be used in secure call flows.

Protocol Capture Warning (Exam Critical)

Situation	Risk
Protocol captures enabled for trunk diagnostics	System does **not encrypt data** — all data including secure flow inputs is logged
PCI DSS setting enabled in org	Genesys Cloud **automatically disables** Media Capture and Protocol Capture settings
Best practice	Never enable protocol captures while using secure call flows in production

---

Permissions

Permission	Purpose
`Architect > Flow > Add`	Create secure flows
`Architect > Flow > Edit`	Edit secure flows
`Architect > Flow > View`	View secure flows
`Architect > Flow > Delete`	Delete secure flows

Workflow — Agent-Referred Secure Session

Agent on call with customer

↓

Agent initiates transfer (Transfer to Secure Flow action in inbound/in-queue flow)

Note: If supervisor is monitoring, transfer cannot be initiated until monitoring ends

↓

Secure Flow begins — audio masked — recording paused

Agent can no longer hear customer input

↓

Customer enters sensitive data (e.g., credit card number) via DTMF

↓

Secure Flow processes payment or stores confirmation number in secure variable

↓

Return to Agent action executes

Confirmation number passed to agent's script

↓

Customer reconnected to agent

Workflow — IVR-Only Secure Session

Customer calls in — routed directly to Secure Flow

↓

No agent involved

↓

Secure Flow processes sensitive data (e.g., account number, payment)

↓

Disconnect action terminates interaction

Key Takeaways

Topic	Summary
Purpose	Mask audio and prevent recording during sensitive data collection
PCI DSS compliant	Yes — designed for PCI compliance

Topic	Summary
Triggering condition	Any secure action or secure variable consumed in a flow activates secure mode
Two scenarios	Agent-referred (returns to agent after) · IVR-only (ends with Disconnect)
Transfer to Secure Flow	Available in Inbound, Outbound, and In-Queue flows
Return to Agent	Terminating action — passes data back to agent; call disconnects if agent left
Protocol Capture risk	Never enable protocol capture when using secure flows; PCI DSS setting disables it automatically
Bot support	Dialog Engine Bot Flows only (PCI-compliant); Digital Bot Flows must NOT be used
Analytics impact	Secure flow time counts against IVR metrics and agent handle time
Key icon	Visual indicator in Architect showing secure action/variable in use

Revision #1
Created 13 March 2026 17:48:29 by Cesar Gzz
Updated 13 March 2026 17:48:35 by Cesar Gzz