ASSERTION®
Collaborate Confidently

ASSERTION® Identity Assurance™ Data Governance Policies

Document Version: 2.0
Date: 9-June-2025
Document ID: PS00P040

Document Revision History

Version	Change Description	Date
1.0	First Public Release	15-Jan-24
2.0	Second release	9-Jun-25

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Assertion Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer

Assertion Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Assertion Inc. Customer and/or End User agree to indemnify and hold harmless Assertion Inc, Assertion Inc' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Assertion Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Assertion Inc does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Assertion Inc support

Assertion Inc (operating as ASSERTION™) provides a channel for you to use to report problems or to ask questions about your product. For support information, see the ASSERTION™ Web site: https://assertion.cloud/support

ASSERTION® is a registered trademark of Assertion Inc.

Contents

Purpose

This policy defines the governance framework for data collected, processed, and accessed by Identity Assurance, a product of Assertion. The objective is to protect the interests of Assertion's Enterprise Customers (Enterprises) and their End-users, while maintaining compliance, integrity, confidentiality, and availability of all data assets.

Scope

This policy applies to:

- All data interactions between Assertion, its Partners, Enterprise Customers (Assertion's or Partner's), and End-users.
- All deployment models of Identity Assurance (on-premise and cloud).
- All employees, contractors, and sub-processors of Assertion who may access such data.

Data Privacy and Security

- Identity Assurance is built to support compliance with:
  - CCPA (if End-user data from California is processed)
  - India's Digital Personal Data Protection Act (2023)
  - GDPR (if End-user data from the EU is processed)
- Features include:
  - Customer preference logging and evidence
  - End-user data access and erasure support
  - Configurable data scopes and retention windows

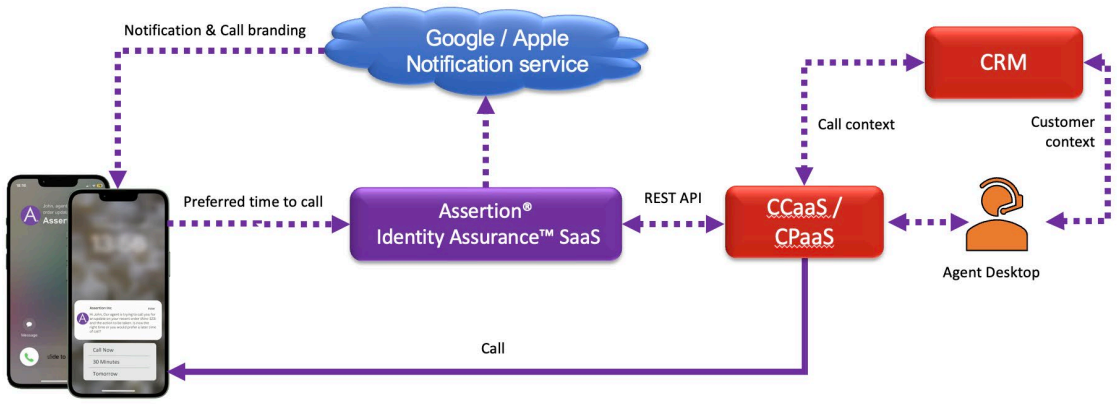
Policy Review & Governance

- This policy is reviewed quarterly by Assertion's Data Governance Council.
- Customer-specific requirements may be appended via Statement of Work (SOW) or DPA.

Cloud Solution

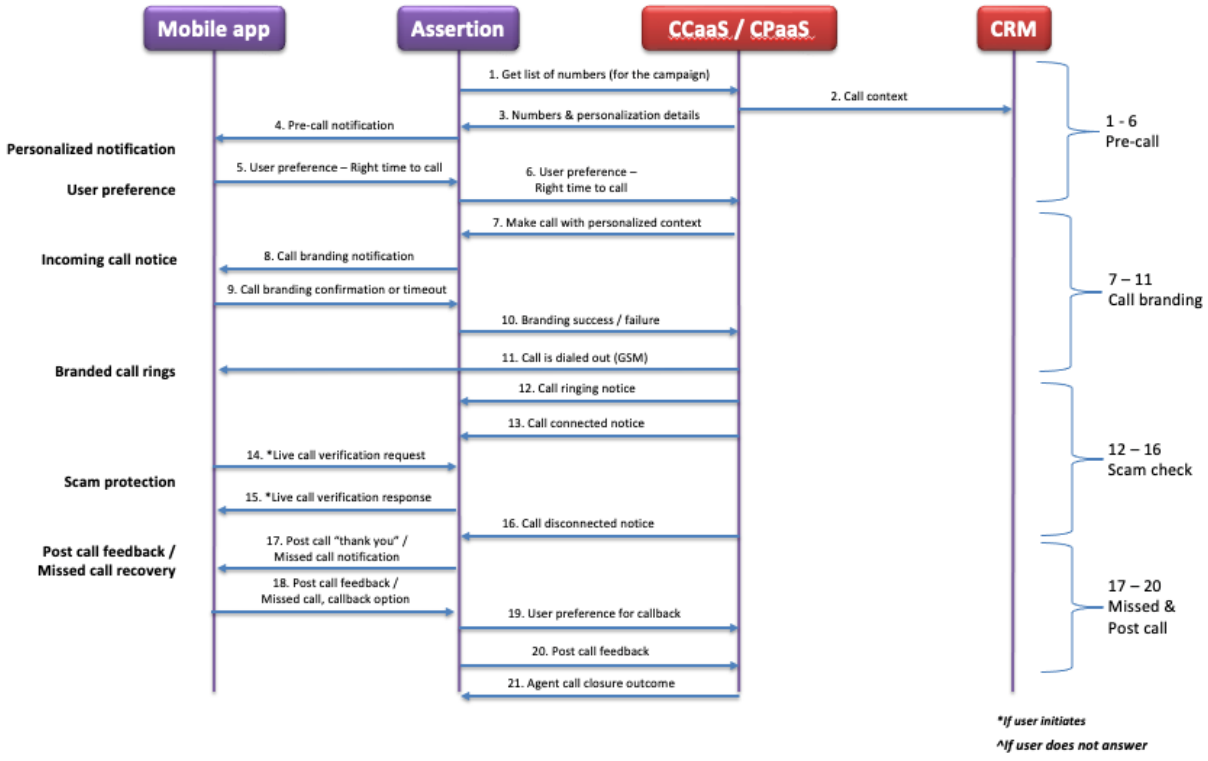
Assertion aims to minimize data collection and processing, especially of personally identifiable or other sensitive information.

How Identity Assurance™ Works – CCaaS Architecture



1. Integrate using REST with your CCaaS / CPaaS provider
2. Mobile app integration
3. Dialer integration for user preference on right time to call & lead recovery (optional)

How Identity Assurance™ Works – CCaaS Call Flow



Key Data Flows and Responsibilities

Operational Flow

1. Enterprise Customer embeds the Identity Assurance SDK into its mobile application.
2. Before initiating a call to an End-user, the Enterprise Customer application backend sends a trigger message (which may include Personally Identifiable or Commercially Sensitive information) to the Identity Assurance service.
3. Identity Assurance notifies the End-user via the mobile app and awaits a response.
4. The End-user response is relayed back to the Enterprise Customer application backend, which uses it to instruct the telephony layer to proceed or defer the outbound call.
5. Identity Assurance may also receive call disposition data from the Customer, including:
    - Whether the call was answered (pickup: yes/no)
    - Call duration (length)
    - CRM campaign metadata
    - Identity-related transaction history

Roles & Responsibilities

- Enterprise Customer (Data Controller): Determines purpose and means of End-user data processing. Owns CRM, campaign, and call-related data.
- Assertion (Data Processor or Sub-processor): Processes data on behalf of Customer per contractual terms and deployment model.

Data Hosting and Access

- Data is stored in cloud servers, currently in the AWS US East Virginia data center, which is our default location.
- Assertion's Access:
    - Full operational telemetry and integration data
    - Limited to the information sent to us in the API
        - Customer phone number
        - Optionally
            - Based on values filled into the "variables" provided
    - Access to PII, CRM metadata, call outcome data, and system logs

Encryption and Security

The service uses TLS 1.2 with ECDSA 256 (RSA 3072 equivalent) encryption for the highest security of data during transit. Data at rest is encrypted using AES-128 encryption. All connections between components are via secure channels – SSH and HTTPS.

Access Restrictions and Audit Trail

Data stored on Assertion cloud is encrypted and under role-based access control. Only authorized service staff can access the detailed reports, evidence trail and raw data. All accesses made by our services and support staff to read sensitive data will be logged in the Audit trail system.

Data Storage

In the Cloud deployment model, Assertion follows a data-walled garden approach where each customer's data is stored in a separate area on the Cloud. This ensures that there is no chance of data from two or more customers being mixed up or incorrectly accessed, thereby ensuring utmost confidentiality and privacy.

On explicit request from Enterprise Customer for data deletion, all the collected data and reports will be deleted from the cloud servers.

Data Categorization and Retention

- Customers can configure which fields are transmitted via the SDK or API.

The data used for delivering Identity Assurance functionality is categorized as below:

- **Raw Data:** Depends on the telephony layer systems. Refer to the appropriate integration document for details.
- **Processed/ Intermediate Data:** The data collected as tokens (or parts of) logs may include
    - Phone numbers
    - Date and Time when phone calls are made

  The above data is required for end-user call pickup patterns, Assertion-branding versus secondary branding analysis, and so on.

- **Report Data:** On cloud, encrypted and stored in a separate bin for each customer

Retention Period

- Raw Data: 30 days
- Processed Data: 90 days
- Reports: 1 year

Incident Management

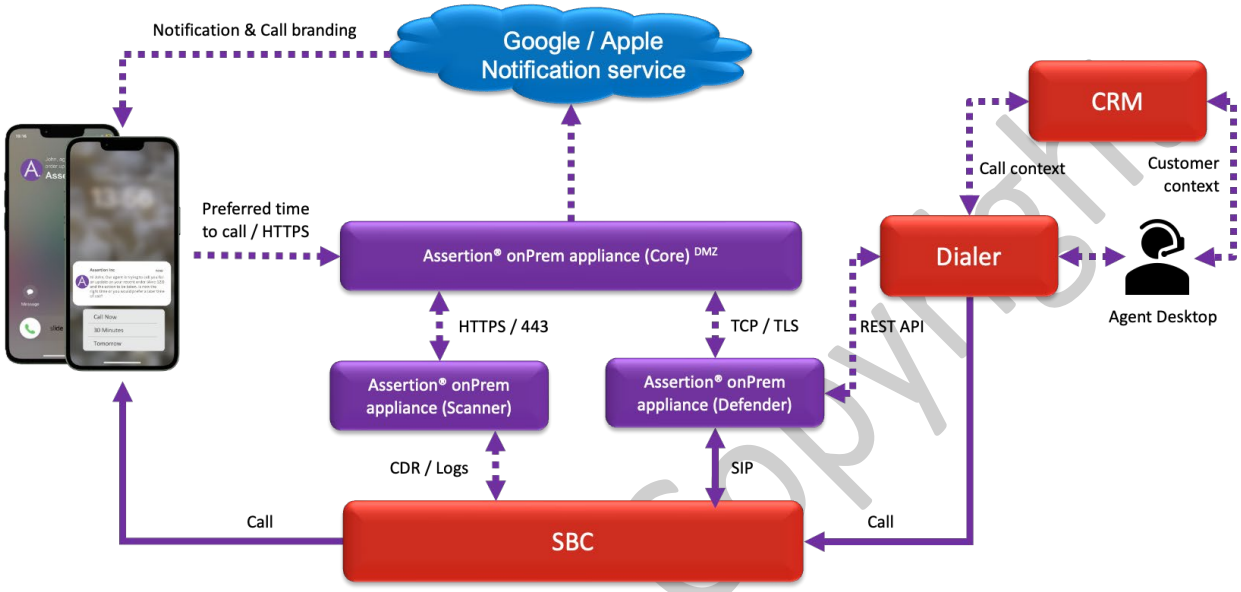
In the event of a data breach:

- Initial notification to Customer within 24 hours
- Detailed incident report within 72 hours
- Root cause resolution and preventive measures documented

On-Prem Solution

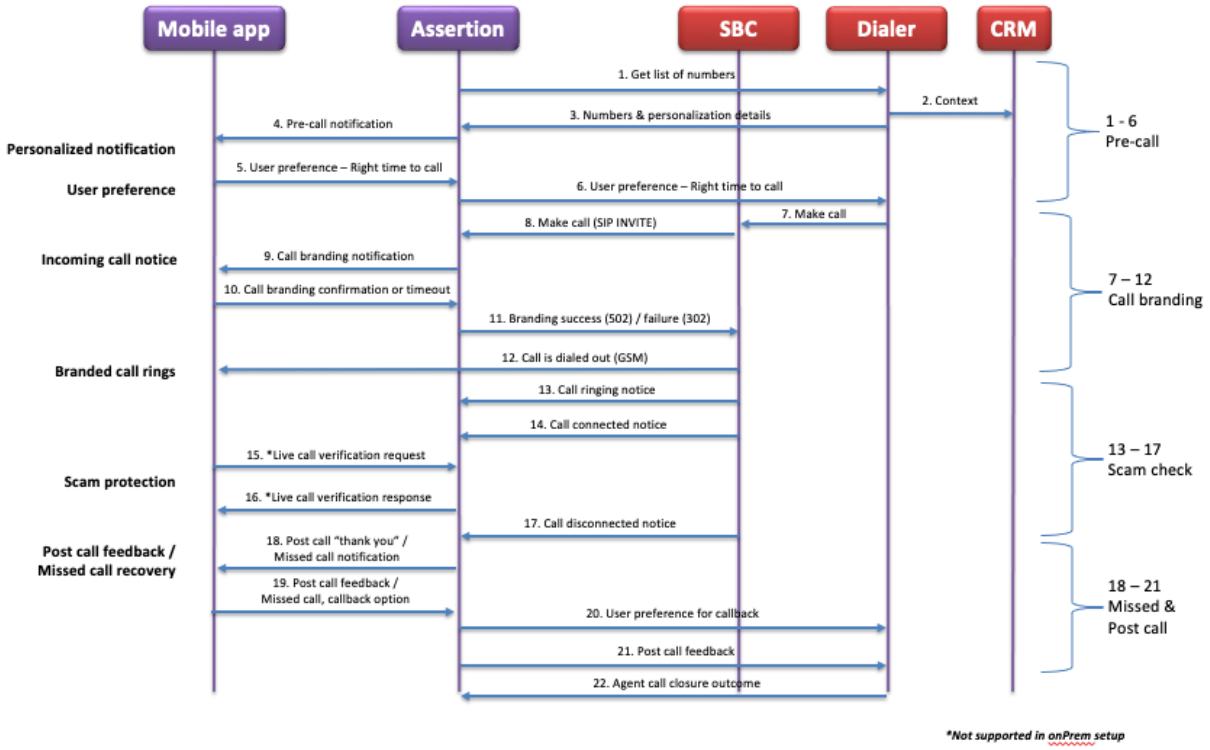
In an on-Prem setup, Assertion does not have any access to Enterprise and end-user data.

How Identity Assurance™ Works – on-Prem Architecture



1. Integrate using SIP with your SBC
2. Mobile app integration
3. Dialer integration for user preference on right time to call & lead recovery (optional)

How Identity Assurance™ Works - Call flow



Key Data Flows and Responsibilities

Operational Flow

Enterprise Customer embeds the Identity Assurance SDK into its mobile application.

1. Before initiating a call to an End-user, the Enterprise Customer application backend sends a trigger message (which may include Personally Identifiable or Commercially Sensitive information) to the Identity Assurance server.
2. Identity Assurance notifies the End-user via the mobile app and awaits a response.
3. The End-user response is relayed back to the Enterprise Customer server, which uses it to instruct the telephony layer to proceed or defer the outbound call.
4. Identity Assurance may also receive call disposition data from the Customer, including:
   - Whether the call was answered (pickup: yes/no)
   - Call duration (length)
   - Identity-related transaction history

Roles & Responsibilities

- Enterprise Customer (Data Controller): Determines purpose and means of End-user data processing. Owns CRM, campaign, and call-related data.

Assertion has no role in this, since Assertion has no access to the on-prem server and its data.

Data Hosting and Access

- Data is stored in the Identity Assurance on-prem server.
- Assertion's Access: Limited to:
  - Deployment support
  - SDK version updates
  - Remote debugging (only with explicit Customer authorization)

Encryption and Security

The service uses TLS 1.2 with ECDSA 256 (RSA 3072 equivalent) encryption for the highest security of data during transit. Data at rest is encrypted using AES-128 encryption. All connections between components are via secure channels – SSH and HTTPS.

Access Restrictions and Audit Trail

Data stored on Assertion Identity Assurance server is encrypted and under role-based access control. Only authorized service staff from Enterprise Customer can access the detailed reports, evidence trail and raw data. All accesses made by Enterprise Customer services and support staff to read sensitive data will be logged in the Audit trail system.

Data Storage

In the On-prem deployment model, data is stored locally on the on-premise servers.

Data Categorization and Retention

- Customers can configure which fields are transmitted via the SDK or API.

The data used for delivering Identity Assurance functionality is categorized as below:

- **Raw Data:** Depends on the telephony layer systems. Refer to the appropriate integration document for details.
- **Processed/ Intermediate Data:** The data collected as tokens (or parts of) logs may include
  - Phone numbers
  - Date and Time when phone calls are made

  The above data is required for end-user call pickup patterns, Assertion-branding versus secondary branding analysis, and so on.

Report Data: In the On-prem deployment model, report data is stored locally on the on-premise servers.

Retention Period

- Raw Data: 30 days
- Processed Data: 90 days
- Reports: 1 year

Incident Management

In the event of a data breach, since the servers are on-prem, it is Customer's responsibility to handle the issue and fallout. Assertion will cooperate fully in investigating the nature of the data breach, treating it as an L1 support incident.