Phase 0: Data Flow Outline

Data Flow Outline

1. **SURGE ID Creation**
   A SURGE ID is automatically generated when a passenger interacts with an existing airport system, such as boarding pass issuance, passport scanning, or Wi-Fi access. The SURGE ID is anonymous, time-limited, and represented as a QR code.

2. **QR Scan Event Generation**
   When a passenger scans their QR code at a defined SURGE zone (terminal entry, security access, customs corridors, boarding gates, transfer points, or amenity access), a scan event is generated.

3. **Scan Event Contents**
   Each scan event contains the following data fields:

   - SURGE ID
   - Zone identifier
   - Timestamp

4. **Scan Ingestion and Temporary Storage**
   Scan events are ingested by the SURGE backend system and stored in short-lived system memory. SURGE IDs are associated with expiration rules to ensure automatic data removal after a defined time period or system exit.

5. **Dwell Time and Congestion Calculation**
   The system compares consecutive scan events associated with the same SURGE ID to calculate dwell time within each zone. Aggregated scan data is used to determine congestion intensity levels across all defined zones.

6. **Decision and Orchestration Logic**
   Based on calculated congestion metrics, the system determines appropriate actions, which may include:

   - Allowing passengers to proceed normally
   - Assigning passengers to virtual queues
   - Suggesting alternate routes or holding areas

7. **System Outputs**
   Decisions generated by the system are delivered through:

   - Passenger-facing browser interfaces accessed via QR codes

- Operations dashboards used by supervisors and staff

8. **Data Expiry and Privacy Enforcement**
   All SURGE IDs and associated scan events automatically expire after exit or a defined timeout period. Only aggregated and anonymized analytics data is retained for system performance analysis.

Conclusion

This data flow outline establishes a clear understanding of how data moves through the SURGE system, ensuring well-defined system boundaries and privacy-by-design principles prior to implementation.