Data Privacy Controls Addendum

This addendum applies to Avaya IX Client SDK Communication Services Package (Android, iOS, Mac OS X, Windows), version 4.4, and later.

Personal Data is stored on the filesystem that is accessible by the current user or as a privileged user. Filesystem content is not encrypted, but may be encrypted using platform technologies. When Personal Data is being transmitted over a network, it is encrypted with the most up-to-date protocols.

Data Categories Containing Personal Data (PD)

- User data (in memory).
  Calls: Remote party phone number
  Conference calls: participant display name, roster list, active talker
  AMM messages: participants on conversation(s), messages
  End user preferences information
  Configuration information
  Contacts retrieved from network (and local contacts application on mobile platforms)

- User data (on disk).
  Local call logs, configuration data or end user preferences are saved on disk. On Windows, users' credentials are saved in in the Windows Credential Manager, in an area that is encrypted such that only the Windows user can decrypt. (Not even administrators.) This area is accessed through Windows APIs. On Mac and iOS, the credentials are saved to keychain. On Android, it is saved in user preferences.

- User data (logs)
  User handle/email, SIP user name, display name information from SIP messages. Virtual room information is saved. Active talker changes. AMM message content or passwords are NOT saved.

PD Human Access Controls

User data (in memory)

- None.

User data (on disk)

- Desktops: By browsing through filesystem. Mobiles: though debug port or iTunes.

User data (logs)

- Through filesystem access, or by using "Report a problem…" option from the application.

PD Programmatic/API Access Controls

User data (in memory)

- Internal programmatic access.
  External application API for desktops (e.g., headset integration) (named pipe/JSON) - can be turned off.
  Series of "Avaya URIs" are configured on the system such that when clicked from, for example, a browser or Outlook plug-in, the link is opened in Equinox application.

User data (on disk)

- Filesystem access done through OS file system APIs.

User data (logs)

- None

PD "at Rest" Encryption Controls

User data (in memory)

- Not encrypted by Equinox application.

User data (on disk)

- Filesystem content may be encrypted through host platform configuration.

User data (logs)

- Filesystem content may be encrypted through host platform configuration.

PD "in Transit" Encryption Controls

User data (in memory)

- HTTPs/TLS 1.2 to send/receive data with servers
  External app interface done through a local named pipe uses local OS facilities and is not encrypted.
  Implemented on Windows and Mac OSX.

User data (on disk)

- TLS 1.2

User data (logs)

- Email sent as a result of "Report a problem…" is sent using standard email protocols. Log files sent in email as attachment are compressed into a single file and may be encrypted by the user.

PD Retention Period Controls

User data (in memory)

- In-memory data is removed based on use cases. For example, during a call, a call object remains in memory. When the call ends, the object is removed from memory, but a new CallLog object is created.

User data (on disk)

- Permanent until rolled over, or app reset or uninstalled, or until user deletes it from filesystem.

User data (logs)

- Not configurable, but can be manually deleted.

PD Export Controls and Procedures

User data (in memory)

- Not applicable.

User data (on disk)

- Users or admin:
  Desktops: Local configuration, call log, and log files can be copied to an external system.
  Mobile platforms: Local files are accessible through Android debug port, or iTunes and can be copied out of the mobile endpoint to a desktop.
  "Report a problem" serviceability option can be selected to compress and email all local files including configuration and call log files.

User data (logs)

- Desktops: Local configuration, call log, and log files can be copied to an external system.
  Mobile platforms: Local files are accessible through Android debug port, or iTunes and can be copied out of the mobile endpoint to a desktop.

PD View, Modify, Delete Controls and Procedures

User data (in memory)

- Not applicable.

User data (on disk)

- User or admin has access to the files on system (on desktops or through adb on Android, or iTunes for iOS). On desktop systems, the files can be edited.

User data (logs)

- Desktop: Admin has full read/write access to the filesystem.
  Mobile: Access through adb Android debug port or iTunes is possible.

PD Pseudonymization Operations Statement

User data (in memory)

- None

User data (on disk)

- None

User data (logs)

- Not applicable.