Data Privacy Controls Addendum

This addendum applies to Device Enrollment Services, Version 3.0.2.

Most Personal Data items are stored in a database which is access controlled and only accessible from the local host via certificate authentication. Some Personal Data items relating to administrative users are stored in a directory which is also access controlled. Data backups can optionally be encrypted. When Personal Data is transmitted over a network, it is secured with TLS and/or SSH.

Data Categories Containing Personal Data (PD)

Company Profile Data

- Company profile data that identifies Company name, address.
  Location: PostgreSQL database.
- Company contact person data that identifies Company's primary contact person First name, Last name, Email address.
  Location: PostgreSQL database.

User Profile Data

- An administrative user profile data that identified user first name, last name, email address.
  Location: PostgreSQL database.

PD Human Access Controls

Most of the Human Access to Device Enrollment Services is through the administration web pages and REST API that the product provides. Device Enrollment Services a role-based access control facility which enables roles to be defined with the permissions needed by different job roles (for example, Service Provider administrator, Reseller administrator, Auditor etc.)

Operating System level administrative user log in through SSH interface. Administrative access through SSH is secured by allowing login only using certificate.

PD Programmatic/API Access Controls

Programmatic access to PD through REST APIs is via TLS (encrypted) communication links.

Avaya – Proprietary. Use pursuant to the terms of signed agreements or Avaya policy.

PD “at Rest” Encryption Controls

The database, directory and log files containing PD items are not encrypted. However, Linux (the operating system on which the product runs) enables the filesystem as a whole to be encrypted

PD “in Transit” Encryption Controls

Data in transit from and to Device Enrollment Services is protected by TLS and SSH.

PD Retention Period Controls

Personal Data stored in Device Enrollment Services is persistent until manually deleted, except for logs which are rotated. Refer to ‘PD View, Modify, Delete Procedures’ below for more details.

PD Export Controls and Procedures

Device Enrollment Services does not support any mechanism for personal data export.

PD View, Modify, Delete Controls and Procedures

View, Modify and Deletion of PD items stored in the database and directory is a manual task. An administrative user would access the administration web pages provided by the product to perform these actions.

Logs are rotated after a set maximum number of log files have accumulated (oldest logs are purged first).

PD Pseudonymization Operations Statement

NA

Avaya – Proprietary. Use pursuant to the terms of signed agreements or Avaya policy.