whistlelink

Encryption & Hashing, Whistlelink

Hashed data

When storing sensitive data, such as passwords, we never offer two-way encryption as that is vulnerable to attacks; we always hash all the data (not susceptible to the decryption). For this purpose, we use a BCRYPT (10 rounds) hashing algorithm based on Blowfish cipher.

Hashed data we store in our system:

- User passwords
- Case passwords used by whistleblowers to follow-up on their case

Encrypted data

When storing sensitive data that needs to be modified & accessed, we are using two-way encryption algorithms key public and private keys so the sensitive data can be manipulated by Whistlelink users. For this purpose, we use 256-bit AES algorithm.

- Password protected Whistleblower site (optional) - Keys used for encrypting and decrypting are stored in a KMS system at Deutsche telekom.
- Case data - Keys used for encrypting and decrypting are stored in a KMS system at Deutsche telekom.
- Files - Keys used for encrypting and decrypting are stored in a KMS system at Deutsche telekom.
- AppSettings entries that contain sensitive information (see below) - Keys used for encrypting and decrypting are hardcoded in our code

Application Settings

Encrypted keys from the AppSettings table

Application Setting Key	Description
Authentication_DhJwtSecret	Secret key used to issue JWT tokens for the Case authentication
Authentication_LambdaApiPassword	N/A
BACKBLAZE_V1_MASTERSECRET	N/A
SMSAPI_TOKEN	API Key for SMS Provider
SENDINBLUE_TOKEN	API Key for Email Provider
DEFAULT_EMAIL	Default email address for sending emails to Whistlelink customers
REPLY_EMAIL	Sets the Reply To email for Send In Blue - Currently only used for overdue cases
AUTHENTICATION_JWTENCRIPTING_KEY	Secret key userd to issue JWT tokens for the Client & Admin authentication
S3_ENDPOINT_STAGING	S3 Bucket Storage Endpoint for the Staging/PreProd Environments
S3_BUCKET_NAME_STAGING	S3 Bucket Name for the Staging/PreProd Environments
S3_ACCESS_KEY_STAGING	S3 Access Key for the Staging/PreProd Environments
S3_SECRET_KEY_STAGING	S3 Secret Key for the Staging/PreProd Environments
S3_ENDPOINT_PRODUCTION	S3 Bucket Storage Endpoint for the Production Environment
S3_BUCKET_NAME_PRODUCTION	S3 Bucket Name for the Production Environment
S3_ACCESS_KEY_PRODUCTION	S3 Access Key for the Production Environment
S3_SECRET_KEY_PRODUCTION	S3 Secret Key for the Production Environment
STRIPE_SECRET_KEY	Stripe Integration Secret Key
SCANNING_SOLUTION_API_KEY	API Key for our File Scanning integration - MetaDefender
S3_BACKUP_ENDPOINT	S3 Bucket Storage Endpoint for backup
S3_BACKUP_BUCKET_NAME	S3 Bucket Name for backup
S3_BACKUP_ACCESS_KEY	S3 Bucket Name for backup
S3_BACKUP_SECRET_KEY	S3 Access Key for for backup

Unencrypted keys from the AppSettings table

Application Setting Key	Description
WHISTLELINK_EMAIL_SUPPORT	Support email address
VERIFICATION_CODE_LENGTH	Length of the Case verification code
VERIFICATION_CODE_CONSISTS_OF	List of allowed characters used to build the Verification Code
USER_TIME_SPAN_HARD_DELETE	Number of days after a soft deleted user is hard deleted
UPLOAD_FILES_ASYNC	Specifies whether file uploads are don sync or async
SUBSCRIPTION_CANCELDATE_TRIAL_LENGTH	Number of days allocated for a new Trial subscription
SCANNING_SOLUTION_URI	Scanning provider URL
SCANNING_SOLUTION_SCANNING_RULE	Scanning provider rules for scanning & sanitization
SCANNING_SOLUTION_SCANNING_ENDPOINT	Scanning provider endpoint
RESET_PASSWORD_EXPIRY_IN_MIN	Number of minutes available for a user to reset their password
REFRESH_TOKEN_AVAILABLE_PERIOD_HOUR	Refresh token lifetime expressed in minutes
NOTIFICATION_TIME_SPAN_UNREAD_CASEMESSAGES	Timestamp of the last unread messages notification job
MFA_EXPIRE_CODE_INTERVAL_IN_MIN	Number of minutes available for a user to enter their MFA code
MFA_CODE_LENGTH	MFA Code Length
MAX_OPTION_VALUES_MULTIPLE_CHOICE	Maximum number of allowed options on multiple choice controls
MAX_OPTION_VALUES_DROPDOWN	Maximum number of allowed options on dropdown controls
LOGO_TYPE_EXTENSION_WHITELIST	Extension whitelist for logo images
JWT_AVAILABLE_PERIOD_MIN	JWT token lifetime expressed in minutes

IS_PRODUCTION_ENVIRONMENT	Specifies whether the current environment is production or not
INTERVAL_MONTHS_OF_CASES_CHART	Specifies the default timespan for deleting closed cases while registering from the Admin site
FRIENDLY_NAME_GOOGLE_AUTH	Friendly name for Authenticator apps
FILE_UPLOAD_MAX_SIZE_MB	Maximum file size for uploads expressed in MB
FILE_UPLOAD_MAX_COUNT	Maximum number of files that can be uploaded at once
FILE_TYPE_EXTENSION_WHITELIST	Excention whitelist for uploaded files.
FAILED_LOGIN_LOCKED_OUT_MINUTES	Locked account lifetime expressed in minutes
FAILED_LOGIN_ATTEMPTS	Number of failed login attempts allowed until an account is locked out
EMAIL_FOR_SMS_CREDIT_ALERT	Email address where SMS credit alerts go to
DEFAULT_PLAN_ON_REGISTRATION	Default selected plan during the registration process
DEFAULT_LANGUAGE_ID	Default Language id for the system
DEFAULT_DELETE_CLOSED_CASE_NUMBER_OF_MONTHS	Specifies the default timespan for deleting closed cases while registering from the UI
DEFAULT_BRAND_COLOR	HEX color code for the brand color
DEFAULT_ACCENT_COLOR	HEX color code for the accent color
DAYS_WHEN_A_CASE_IS_OPEN_NEW	Specified the low threshold for opened cases
CONFITM_LINK_INVITATION_EXPIRE_IN_HOURS	Confirmation link lifespan expressed in hours
CASES_STATS_NEAR_DEADLINE_PERIOD	Number of days before a Case is considered near its deadline
CASE_NUMBER_LENGTH	Length of Case Numbers

CASE_NUMBER_CONSISTS_OF	List of allowed characters used to build Case Numbers
BYPASS_OPSWAT_RESPONSE	Specifies whether the application requires files to be scanned before made available to users
BIG_PERIOD_IN_DAYS_WHEN_A_CASE_IS_OPEN_NEW	Specified the high threshold for opened cases
BACKUP_FILE_STORAGE	Specifies whether the current environment backs up the file storage
BACKBLAZE_V1_MASTERKEY	N/A
BACKBLAZE_V1_BUCKETNAME_PROFILES	N/A
BACKBLAZE_V1_BUCKETID_PROFILES	N/A
AUTHENTIFICATION_COGNITO_DEFAULT_COGNITO_USERPOOLID	N/A
ADMINISTRATION_EMAIL_DOMAIN	Administration email domain used for sending emails for Cases & Tenant Statistics while on development environment