Data Handling and Encryption of Credentials in TechIDManager

TechIDManager is a product written by Ruffian Software, Inc. to help MSPs manage the multitude of privileged accounts that they need to create and maintain. This allows each technician to have a unique account on every client's network. TechIDManager does this with four pieces that work together and pass information with encryption in a manner such that the only credentials a person can see are their own.

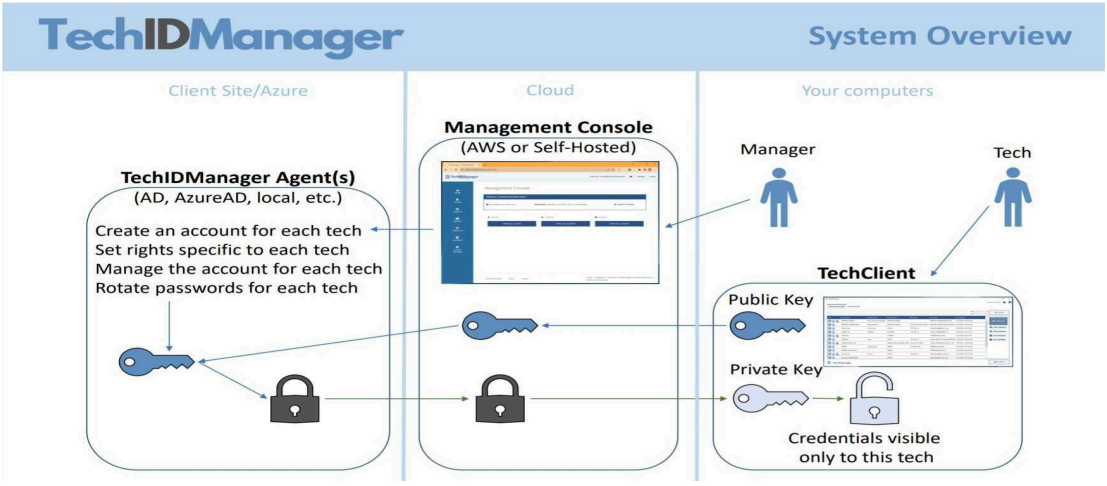
The first piece of TechIDManager is one of a series of agents that runs on the places where accounts are created and maintained. There are managed agents for domain controllers, Azure AD, and local machines. The managed agent creates an account and creates a fully random password. Every 24 hours, the password is changed for every account and every tech. When this happens, the password is encrypted with the public key from an RSA key pair that is specific to that tech. The encrypted version of the credential is then sent via HTTPS to the ManagementConsole; at which point the agent forgets the password. No passwords are stored by the agents anywhere. There are just-in-time agents that work similarly. The just-in-time accounts (JIT) offer the same amount of security but can be activated/deactivated as needed; leaving less standing privileged accounts active.

The second piece of TechIDManager is the ManagementConsole which runs in the cloud. The ManagementConsole is the data storage between TechClient and agents. All information stored in the cloud is stored on an encrypted disk. All credential information that is stored is further encrypted with the specific RSA key of the tech who owns each account. The ManagementConsole does not store, or ever have access to, the Private Key of the RSA key pairs that encrypts the credentials. In this way, no one with access to the data stored in the ManagementConsole can see any credentials. The private keys needed to decrypt a set of credentials only exist on the tech's computer who owns that account.

The third piece of TechIDManager is the TechClient. This is what each tech uses to get access to their credentials. This runs on each tech's computer. Each tech's computer stores the private key from the RSA key pair locally. All locally stored information is stored encrypted with AES-256 encryption, based on a passphrase that the tech has to enter to get access to the TechClient.

The fourth piece of TechIDManager is the asymmetric encryption. This is to ensure that all credential information that is stored is encrypted with the specific RSA key of the tech who owns each account. The Management Console does not store, or ever have access to, the Private Key of the RSA key pairs that encrypts the credentials.

All communication between these three pieces is via HTTPS (with TLS 1.2 or TLS 1.3 depending on system setup) to REST API's. All RSA key pairs are currently 2048 bit.



All information in the document is proprietary information of Ruffian Software, Inc. and should be treated with the respect that you want your proprietary information treated with.

For additional information contact support@techidmanager.com