TRAKA AUTOMOTIVE
FINGERPRINT PRIVACY

Experience a safer
and more open world

WHAT ARE THE RISKS TO USER PRIVACY?

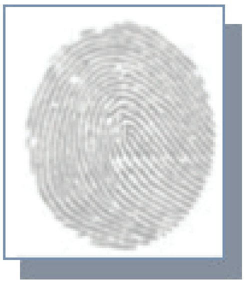
When a fingerprint is scanned only certain points of the fingerprint, such as ridge points called 'minutia', are used to produce a unique template.

Using optical sensors to capture high quality fingerprint images, the readers analyse the fingerprint image and convert it into a series of numbers called a template. It's the template that is saved, not the fingerprint image!

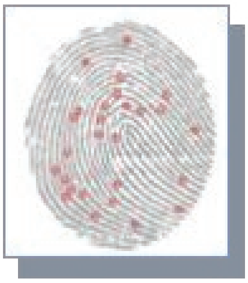
The template is stored within the database for backup & verification purposes and additionally sent to a protected database within the fingerprint reader module attached to the Key Cabinet. The desktop enrolment module does not store any templates and there is no method of extracting the templates from the reader module attached to the Key Cabinet.

The template data stored in the database is that produced by the readers algorithms. We use a secure SQL Server database to protect this data.

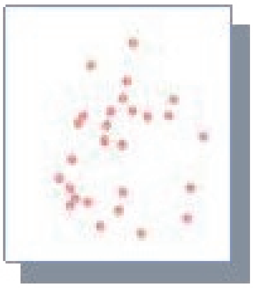
User Places Finger Onto Reader



Reader Sees Image of Finger



Reader Detects Points



Reader Stores Points Only