CSI MOBILE – DATA SECURITY

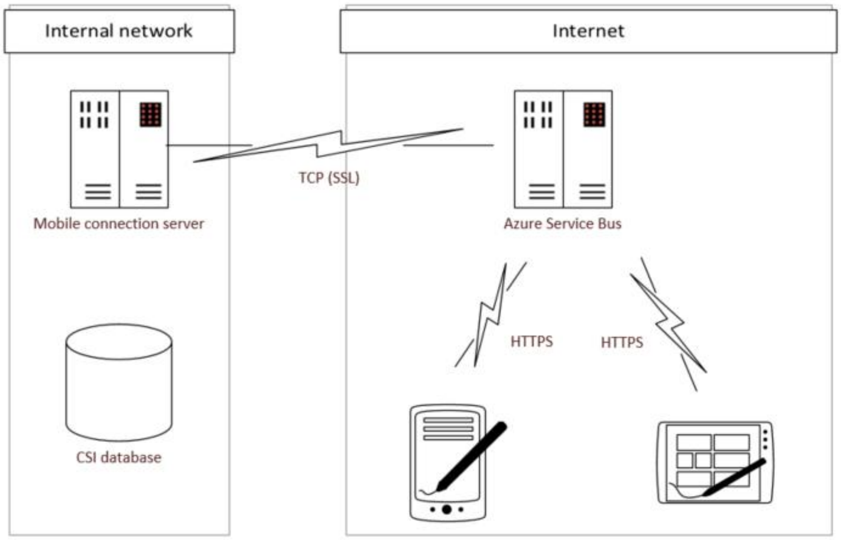
CSI Mobile offers a secure way to make time entries to CSI Lawyer with mobile devices. It utilizes the same encryption technology as netbanks.

The solution is based on the cloud-based Microsoft Azure Service Bus Relay, acting as a link between the CSI server and the mobile device. A connection from the mobile device to the CSI server is created using a Shared Key method. When a Service Bus is accessed by a mobile device whose key corresponds to a key stored on the CSI server, Service Bus establishes a secure connection between the mobile device and the CSI server. All communication between the server, the cloud and the mobile device is encrypted.

The mobile device stores only the user's login information for establishing the connection, and the identifiers of the user's transaction types. Other information displayed in CSI mobile is removed from the mobile device memory when the mobile application is closed.

TECHNICAL DESCRIPTION

CSI Mobile's data security solution utilizes Microsoft's Azure Service Bus Relay technology. Outbound connections established both from the CSI server (located in the internal network) and from the mobile device are connected on the Azure Service Bus server. For more information about the service bus, see http://azure.microsoft.com/en-gb/services/service-bus/.



ESTABLISHING A SERVICE BUS CONNECTION

In order for the Service Bus to communicate securely between the mobile device and the CSI server, they both must be authenticated to the Service Bus service. Here, the Shared Key method is used at both ends. The shared key is formed at the end of the Azure Service and transferred to the customer during installation. The key is too long for entering it manually to the mobile device, so it is temporarily stored in the Azure service when registering the device. The service transmits the key to the mobile device using one-time access codes.

REGISTERING A MOBILE DEVICE

When registration starts, the mobile device retrieves a verification code from the registration service and asks the user to enter it into the CSI software on the desktop. Once this is done, the CSI software in turn retrieves a verification code from the registration service and asks the user to enter it into the mobile device. The shared key is stored on the mobile device after the registration process has been successfully completed.

AUTHENTICATION OF THE CSI SOFTWARE

When registering, the mobile device asks for the identification information with which the user logs into the CSI software. The same IDs also serve as CSI Mobile IDs and are stored in the mobile device for further use. If a user logs on to CSI with a domain account, he/she must set a separate ID and password for CSI Mobile.

SERVICE REQUEST STRUCTURE

For authorization, the server requests have three Authorization headers. The standard authorization token covers a Shared Access Signature for Service Bus, created using a shared key. The “AuthCSI” token covers the authorization information for the CSI software and the “DeviceID” token for the device identification. For each request, all these tokens will be sent to ensure that: a) the device is registered with Service Bus, b) the user is identified in the CSI software, and c) the device is registered with the CSI software for that specific user.

REMOVING THE DEVICE REGISTRATION

The CSI Mobile application registration can be removed from the mobile device in the Settings. If the mobile device is lost, its registration can also be removed from the CSI software (user's data) on the workstation. The mobile device will then have no access to the CSI software information until the device is re-registered.