Increase Equipment Availability

+ Hotline with experts to provide remote mechanical, process, and software support
+ Real time and complete diagnosis with multimedia tools (Chat, Webcam, Whiteboard)
+ Excellence United experts respond quickly to service issues without waiting for a technician to arrive on site
+ Qualified and complete preparation for service visits

Avoid Unplanned Downtime

+ Quick identification of critical components
+ Condition monitoring
+ Preventative maintenance tools

Maximize Production Flexibility

+ Reduce changeover times
+ Optimally trained operating personnel
+ Visual support for machine setup

With the Excellence United Service Portal, support requests are simply and easily made directly from the machine HMI

Your package includes
- Remote diagnosis/teleservice/firefighting
- Conference center
- Machine documentation
- Spare parts catalog
- Maintenance manager
Everything for your IT security

Connection
A connection is only possible as a reconnection following a service request which was initiated by the customer. After closing out the service request, the connection can only be re-established by placing a new service request. The customer can close the connection at any time. The “Access Guard” allows an optional single approval of functions.

Safety
The system is based on a SSL encrypted client-server connection. Similar to home banking, a connection is only possible if the client trusts the server and knows its certificate. The difference to classical home banking is that the Service Portal requires an additional verification of the client’s trustworthiness by the server. The login via the encrypted connection only becomes possible after successful verification. The system meets the requirements applicable to remote maintenance in an industrial environment in compliance with the directive BSI-CS 108.

Communication
The customer server communicates exclusively via SSL/TLS Port 443 TCP. In the firewall, the communication can be restricted to just one destination address. At no time, will a connection be established via another port – neither incoming nor outgoing. The customer server connection with the central server can also be established via a local proxy. When remote desktop programs or programing tools are used, application-relevant, point-to-point connections are established between the client’s computer (service technician) and the target (machine network) only for the duration of use (e.g. between the Simatic Manager, established on the service technician’s computer, and the target control system). Unlike other normal VPN connections, use of this connection by other programs for other targets on the client’s computer is not possible.

Log data
All relevant user actions are stored in a tamper-proof LOG file.

Encryption
The transport encryption is realized with public key RSA 2048-bit. Symmetrical encryptions use AES 256-bit.

Authentication
Authentication is realized via role-specific SSL certificates. Every user receives a specific login with password. Adaptations and extensions in the authentication can be tailored to a customer’s in-house requirements.