

Mobil'Itium

Management and securement
of roaming profiles

Simplify nomad user access from
all the thin terminals installed
in the enterprise.

Encrypt and protect the user
authentication data by means
of a confidential code (PIN).



Mobil'Itium, integrated on a USB pen, is a solution for the authentication of roaming users from Itium thin clients. Mobil'Itium simplifies and secures the roaming access to confidential and personal data from any Itium thin client on an enterprise network. This solution thus meets the mobility needs of personnel who have to move constantly from one workstation to another, for example, nursing personnel in hospitals or clinics.

Dynamic configuration of Itium thin clients

The access key on Mobil'Itium USB pen allow the dynamic configuration of the Itium thin client according to its user (profile, servers used, domain, work area, etc.) The authentication data are protected by an AES 128 bits strong encryption and a four-digit confidential code (PIN).

Inserted in the slot for opening the thin client session, Mobil'Itium USB access key applies in a dynamic manner the configuration profile corresponding to the user, taking him immediately to his work area and the documents he is authorised to access.

Moreover, having a storage capacity from 512 Mb to 1 Gb, the Mobil'Itium can be transformed into a complete pocket desk. Using a generic Windows driver, Mobil'Itium allows fully transparent use of the functionality for local saving on USB peripherals, implemented in the Itium thin clients. When the Mobil'Itium key is disconnected, the Itium thin client returns automatically to its initial configuration, ready for another roaming user.

Simplicity in administration and traceability

The Mobil'Itium keys on USB pens can be administered easily from the centralised administration, the ItiumAdmin interface. The integrated configuration wizard allows an easy definition of user profiles and associates these profiles with access rights to the server systems. The enterprise thus exercises an improved control regarding access to its resources or confidential data, such as the patient files in a hospital. Through a more secure identification of the users, the Mobil'Itium solution also allows satisfying the mandatory requirements of traceability with regard to modifications as well as the consultations of data considered sensitive.

Management of roaming users

The user has a USB key on which are saved his connection profiles (sessions RDP, ICA) as well as his authentication data: User name, Domain, Password. The authentication data are encrypted and are protected by a four-digit code (PIN).

When the key is inserted an Itium thin client, the user is prompted to input his PIN code and has three attempts after which the sensitive data are deleted.

The session profiles are then loaded into the Itium Thin Client and can be run automatically.

The authentication data are transmitted to the server for establishing the connection without any other intervention being necessary.

When the key is removed from the Itium, the current sessions are disconnected, offering thus the possibility of reconnecting from another workstation without loss of data. The session profiles are deleted from the Itium Thin Client.

Data storage medium

The USB key remains a classic storage medium accessible by the user directly in his Windows session for transporting his personal data.

Deployment tool

When the key is inserted in the Itium Thin Client, an intuitive interface allows moving the session profiles between the Thin Client and the key for defining the profiles that shall be loaded dynamically.

Technical Characteristics

USB 2.0 key, 512Mb or 1Gb Flash memory.

Encryption: AES 128 bits