



Full mobile Identification and Authentication solution: mID – Mobile IDentification component Authentication Server

mID

Located at the point of sale, the mID is an identification and authentication physical component for mobile handsets. The identification and authentication are used for various applications, predominantly for mobile payments.



Authentication Server

Located at the backbone of the network, AcCells' authentication server authenticates the mobile phones with the mobile network security scheme and, as an option, with the mobile account balance and rights.



Key Benefits:

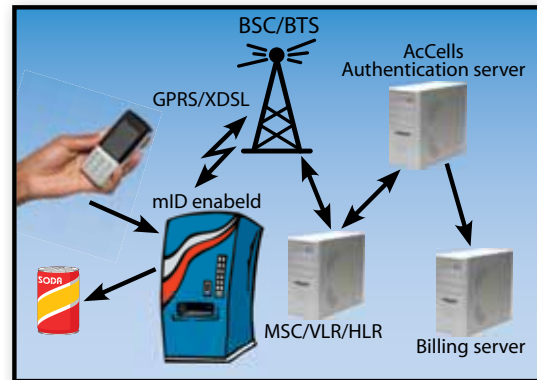
- Simple to use, Fast, and Accurate
- GSM bullet proven security
- No need for SMS or data plan
- Works with every existing phone
 - No hardware upgrade
 - No software installation
- Low rollout CAPEX and OPEX

Features:

- Using Near field GSM signaling
- Syncing the mobile phone to a monocell
- Single mobile device support per mID
- Can be part of the cellular network
- mID: Internal / External (add-on) component
- Multiple operators support
- Multiple mIDs per backbone link support
- Fast authentication time
- Cellular networks support: GSM 2G, 3G
- Backbone ports: Ethernet, GPRS / HSDPA
- USB port
- mID transmission received only inside the mID
- Configuration and management
- Authentication methods:
 - SIM base authentication (IMSI)
 - Device base authentication (IMEI)
 - PIN code
 - Cellular network authentication
- Authentication during active call (future versions)
- Multiple device connection protocols
- Various network servers protocols
 - AcCells CAMEL phase 3 authentication server
 - Credit card authentication aggregator
- Real time authentication transactions and periodic billing transactions
- Device drivers for the mID

● **Simple, Fast, and Accurate.** The mID enables intuitive operation, credit card like, which identifies the mobile handset and approves the receipt of the service / goods.

● **GSM bullet proven security.** Authentication: the authentication method used by the cellular network, cross region and cross provider. Integrity: the data arrives without any modifications. Confidentiality: the radio channels are secured in order to transmit information. Device Security: if a device is stolen, the PIN code and the authentication will result in a failure.



MNO installation system diagram

● **Works with every existing phone.** The mobile handset is identified by the basic cellular network mechanism. This is why even a ten year old basic phone, without any software update capabilities, can enjoy all the mID applications.

● **Free identification and authentication transaction direct costs** due to the usage of the free GSM basic signaling. No other GSM service is needed other than the mobile payment.

● **Low rollout CAPEX and OPEX.** Using the existing mobile handsets, the deployed network signaling service, and a scaled CAMEL server architecture, enable progressive rollout (pay as you grow) of mobile payment services with low CAPEX and OPEX.

● **mID Applications.** The mID enables many devices ('applications') with mobile identification and authentication capabilities. A common device is a POS machine. mID applications are not limited to physical goods payments, from heavy vehicle keys to web transactions security device – the possibilities are endless.

AcCells

AcCells was launched by seasoned and prominent technologists to commercialize a breakthrough innovation that lays the foundation for a new paradigm in mobile payments. Our vision is to create an infrastructure which will stimulate the growth of mobile payment applications worldwide. AcCells will pave the way for industry growth by sidestepping the enormous cost of upgrading while expanding the potential end user market.

