DEVICE GRID

Secure, scalable connectivity intrastructure
for Internet-enabled devices

Trifork's Mobile Device Grid (MDG) provides scalable secure connectivity for mobile applications and IoT devices.

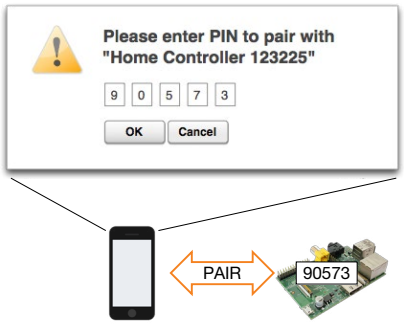
The product consists of a set of client modules that can be integrated into embedded devices or mobile applications and an accompanying cloud service that provides connectivity across network protection boundaries such as NAT routers.

Privacy

Using industry standard Elliptic Curve Cryptography and end-to-end TLS/SSL security, MDG safe guards against privacy issues and 3rd party snooping.

The system has no back door; the MDG cloud servers cannot observe or change the contents of messages transmitted between paired devices.

MDG uses a familiar access pattern known from Bluetooth devices: A user authorises a pairing of two devices using a pin code. After such a pairing, the two devices can reach each other locally, or remotely by indirection of the MDG cloud service.



Availability

Once paired, two devices can interact with no Internet connectivity using LAN or WiFi technology.

Key Features

- Supports iOS, Android, Windows Mobile
- Local or LDAP based user administration
- Unlimited number of apps and versions
- Unlimited number of users and groups
- Detailed crash reporting and crash statistics
- Detailed analytics information
- Provide rich feedback from end users directly to developers
- More hosting options
- Supports leading X-platform technologies

TRIFORK.
...think software

DEVICE GRID

The cloud services are hosted in multiple locations allowing the system to provide very high availability.

Scalability

Depending on need, the MDG cloud services can be deployed with geo-scaling, which allows improving connection speed.

Shared hosting infrastructure, allows MDG to provide a very attractive cost per unit for connected devices.

Integration

Developers can use the MDG client API's to establish connections securely passing any kind of messages or data across these channels.

Clients Modules

Client software is available for integration with the following platforms:

» iOS 7
» Android 4
» Windows Phone 8
» Linux and BSD-based Platforms

Other platforms available on request.

The client module can be linked into client applications, or run as a separate service available via on-host IPC mechanisms.

The client module requires network access, and a working memory of 1-2MB.

Security Technologies

In the default configuration, Trifork MDG uses TLS with EC/ECDH based on the elliptic curve BrainpoolP320r01 (320bit keys). Other configurations are available. Pairing uses standard PAKE protocols.

Encrypted sessions are established end-to-end. The MDG cloud services only enables peers to find each other, peer-to-peer connection establishment and traffic routing.

Privacy

Both peers and cloud infrastructure can be configured to provide varying levels of privacy depending on customer needs. A primary criterion for many customers is that MDG traffic should not reveal information that can be used to establish a user's current physical location.
For management and customer support however, it may be desirable to selectively keep records of certain interactions for a limited time.

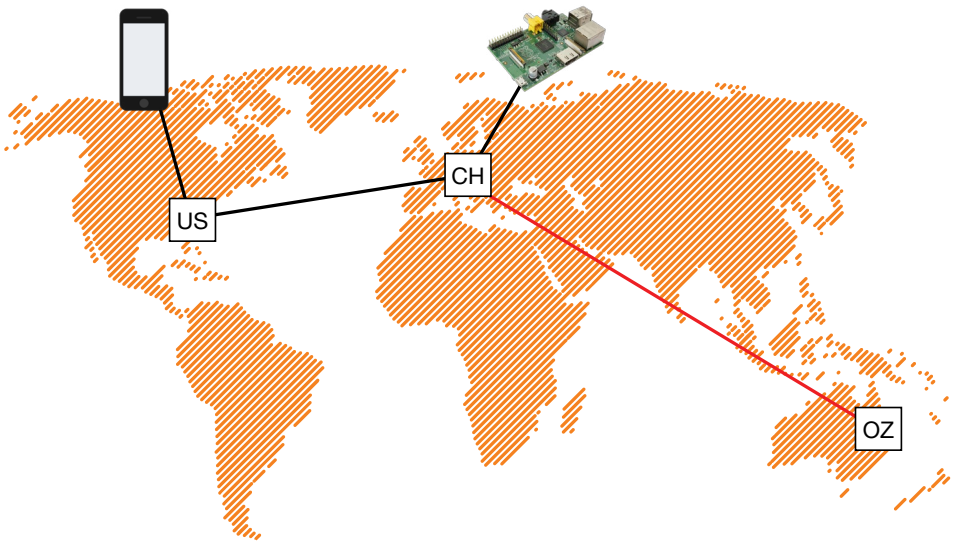
Thorough security model documentation is available upon request.

Optional Components and Services

Integration services for applications and embedded devices.

Management and support console applications.

Custom security configurations.



Want to know more?

Business Development Manager
Maria Wennestam
maw@trifork.com

Software Pilot
Andreas Frish
afr@trifork.com

TRIFORK.
...think software