



QwyitFone™

Secure Voice

BUSINESS AND TECHNOLOGY PRESENTATION

Business Concept

Problem – Market Summary

- ▶ There is no way to make a cellular secure voice communication call
 - ▶ GSM, the worldwide, largest voice network, is hacked (both A5/1 and KASUMI)
 - ▶ “GSM has not been changed much, since to do so would require reprogramming phones, cell towers, and networks around the world. ”
 - ▶ IDEN and CDMA in the US are just as insecure (CAVE/CMEA/ORYX hacked as well)
- ▶ Options for VoIP calling networks (WhatsApp, Signal, etc.), but not cellular
 - ▶ Some sort of data plan is required
 - ▶ Not all phones support mobile VoIP software
 - ▶ Call quality differs between wireless carriers
- ▶ **QwyitFone™** Solution: provide the same proven VoIP security over cellular networks
 - ▶ Secure Voice: Worldwide, uniform service over **any cell network**

Business Concept

QwyitFone™ secure voice app

- ▶ **QwyitFone™**, Android smart phone communication
 - ▶ By 2020, 6.1B smartphones, nearly 70% of all mobile devices
 - ▶ Q4 2015, of the 432M smartphones sold, 352M ran Android (81.7 percent)
 - ▶ Android Operating System Project OS code for smart phone voice communications
- ▶ **QwyitFone™**, the world's first globally secure cellular voice communications
 - ▶ No performance degradation or complexity (like Signal)
 - ▶ No special switches or network intrusion (like Cell Crypt)
 - ▶ Simple app download and immediate secure operation w/QwyitFone™ callers

QwyitFone™: 256-bit authentication and encryption over cell networks

Business Concept

QwyitFone™ is the Solution

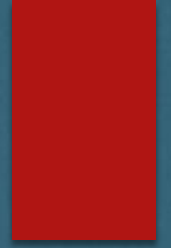
QwyitFone™ is the world's first authenticated, encrypted secure cellular Voice Service

- ▶ QwyitFone™ is part of the QwyitTalk™ centralized security *Service*
 - ▶ Better security, performance, uniformity, ease of use, integration, proliferation – network independent
- ▶ QwyitTalk™ replicates, extends, enhances and unlocks the VoIP TLS security model by changing the underlying *method*
 - ▶ TLS relies on PKI methodologies that don't work for today's Cellular communications networks
- ▶ QwyitFone™/QwyitTalk™: Fast, Small, Efficient, Simple, Flexible, Secure

Competition

- ▶ There are no network-independent authentication and encryption services for cellular voice communications
 - ▶ Current underlying methods broken and insecure
- ▶ VoIP secure calling apps
 - ▶ Signal, WhatsApp, Cellcrypt, etc. all use Transport Layer Security (TLS)
 - ▶ Same security process provided by a locked browser HTTPS connecting with a web server
 - ▶ TLS is a proven security process, but cannot be ported to a cellular network
 - ▶ Performance degradation such that calls wouldn't work
 - ▶ Complexity of the TLS model
 - ▶ Every network switch would have to be 'enabled', the same way that web servers over the Internet require individual PKI certificates installed: this cannot be done

Qwyit LLC



- ▶ 10 Patents Granted (9 US, 1 Japan), 1 Patent Pending (These are the latest):
 - ▶ [US 2016/0301672](#); [US 9,374,347](#); [US 8,649,520](#); [US 2012/0260087](#); [Japan 5047291](#)
- ▶ 30+ White Papers (technology, application, marketing, documentation)
- ▶ Reference Software (test vectors, bias testing, primitives)
- ▶ 7 different example (historical) applications
- ▶ Production SDK Toolkits (Java, C++, C)
- ▶ FPGA Hardware investigation and Verilog code

Opportunity



Qwyit LLC is looking for a technology/business partner to accept an exclusive license to build/operate/benefit from the operation of QwyitTalk, Security as a Service

Contact us

Info@qwyit.com