# Qwyit™

## True Cryptography Innovation

BUSINESS AND TECHNOLOGY PRESENTATION

# Introduction
## The Insane Digital Security Industry

**'Insanity is doing the same thing over and over and expecting different results.'**

- Nothing is more tragic than the *entire digital security industry* continually creating, offering and adamantly insisting on using the same constantly failing fundamentals

***It's time for True Cryptographic Innovation!***

# Security Market Issues

Security technologies aren't used in every communication, in every digital application, they aren't baked into the multiple device architectures across all the various digital networks. If they were, almost all of the problems – from network intrusions to financial fraud – would be, if not solved, severely limited.

***Why isn't everything secure?***

- There's no universal, simple, fits-everywhere method
  - Current methods are: too big, too complex, too slow, too insecure
- Networks have become multi-dimensional
  - End-to-end authentication/encryption is impossible w/current methods

# Qwyit® Solution

Digital presence desperately requires:

Truly universal, constant mutual authentication and provably secure encryption that fits everywhere across all networks, is simple, and works the same way – everywhere!

And…a New Model for marketplace penetration: because security is 'expert stuff', and the software market is 110% over-saturated with a cycle of never-ending 'Best Practices', just rearranging chairs on the Titanic of impractical current methods.

- Qwyit's plan: Hardware Security, our QwyitChip™.

# Value Proposition

According to Market Research, the global Hardware Security Modules Market was valued at USD 581.05 million in 2017 and is projected to reach **USD 15.20 billion by 2025**, growing at a CAGR of 12.8% from 2018 to 2025.

- https://www.marketwatch.com/press-release/global-hardware-security-modules-market-size-and-forecast-to-2025-2019-10-09

What is a Hardware Security Module?

- "Hardware security module is defined as a physical computing device that is used for safeguarding and managing digital keys for strong authentication and providing crypto processing. "

**This entire market is based on using current, ineffective security methods that are the cornerstone of the de facto-failed S/W approach of the last 50 digital-era years.**

**Qwyit's universal, world's fastest encryption chip, QwyitChip™ and the accompanying, identical QwyitSDK™ software module, replaces the need for external, separate, ineffective, costly new H/W.**

# Summary Value

Digital Communication marketplace has recognized their 75-year failed software approach for digital security (Good!)

- The CyberSecurity solution is to offer an encapsulating Hardware solution (Good!)
  - The solution is to replicate the same failed software techniques in costly, cumbersome, complex, separate Hardware add-ons (*Very Bad!*)

**Qwyit has the superior, proven hardware solution using a new, world's fastest encryption technique in an FPGA (QwyitChip™ - Very Good!)**

- Small component of existing device architectures that can simply be incorporated
- Ultra-low cost, zero complexity (it just works), 100% compatibility anywhere/everywhere

The market has already demonstrated the massive potential of the FPGA-centric technology model: Intel's $16.7B purchase of Altera's superior FPGA technology platform in 2015

- The FPGA HSM market opportunity is wide-open, and of immense value.

# Business Plan

*Corporate Mission* is to create/build the QwyitLab™ as a demonstration laboratory for superior Qwyit™ security technology proliferation

- Exactly as the well-known Dolby™ Labs was created/succeeded in proliferating their superior component sound technology by creating/introducing it into marketplace areas by building prototype sound products and demonstrating these to marketplace participants, we will do the same with our superior component Qwyit™ cyber-technology by creating/introducing it into data communications/storage marketplaces initially; financial and other marketplaces in future

*Business Model* is licensing the technology, in all possible formats/models, to market participants (new and existing) for them to build/produce the as-demonstrated Qwyit™-enabled superior security products and services

# Current Product Focus

*Initial Focus* – The QwyitChip™ industry: Introducing a superior H/W security Module (FPGA) into the $15B Hardware Security Module marketplace

- Minimal marketplace hurdles - our solution is a new *internal* HSM
- Our exact design/protocol results are the pre-requisites to new H/W: SPEED and EFFICIENCY
- Our accompanying QwyitSDK™ and QwyitKey™ components allow simple, straightforward operation/support for the new QwyitChip™ Secure cyber-frontier.

*Patented and Prototyped – The Security System for Any/All Network Communication*

- **QWYITCHIP™** – The entire Qwyit™ authentication and encryption service on an FPGA
- **QWYITSDK™** – The identical QWYITCHIP™ capability in a SDK
- **QWYITKEY™** – Participant-managed, independent-trust Authentication Service

# QwyitChip™

- Tested and Verifiable on FPGA Altera DE5
  - FPGA 100 MHz
  - 7 clock cycles
  - Latency 70 nanoseconds
  - 14 MHz Throughput
  - 0.5 Gigabytes per second
  - SLOC – less than 500
- Next-Generation designed for Application Specific Integrated Circuit (ASIC)
  - 1000 MHz
  - 4 clock cycles
  - Latency 4 nanoseconds
  - 2500 MHz Throughput
  - 32.768 Gigabytes per second

To put these performance numbers in perspective:

- Intel's fastest AES software encryption (using a hardware accelerator chip running at 3.33 GHz) requires 5.7 cycles/BYTE to encrypt at 0.5 GB/sec
- Using the same implementation, QwyitChip™ would encrypt at 110 GB/Sec. This is **over 200 times faster!**
- And...Provably Secure (mathematically, not bit-fiddled like AES in CBC mode)

# Technology – Benefits

**Qwyit™ delivers security perfection with the required, real-world properties:**

## Fast, Small, Efficient, Simple, Flexible, Secure

- **FAST** – several *orders of magnitude* **faster than all current methods**
- **SMALL** – The entire SDK is less than ***10KB in software***; fits on **any device** in hardware
- **MORE EFFICIENT** – ***orders of magnitude*** in bandwidth, dev space, msg architectures
- **SIMPLE** – Underdetermined, in **4 Qwyit™ instructions: MOD16, Combine, Extract, XOR**
- **WIDELY FLEXIBLE** – Multiple unique products across **multiple markets, ready for adoption**
- **MORE SECURE** – Mathematic proof, Quantum-ready, ***continuous, mutual authentication in every transmission in real time***
  - Includes two cryptographic science innovations that ***do not exist in any current techniques***:
    - Qwyit™ delivers true, mathematically independent, provably secure OTP encryption: *unique key bit for every plaintext bit*
    - Qwyit™ delivers a method for instant key update uniquely at every use with NIL (no) communication between any users; the Holy Grail of key management – instant, undetectable, at any time

# Technology – Qwyit™ Compared

*GREEN highlights* where there is a demonstrable, substantial market advantage/improvement
*RED highlights* where there is a demonstrable, substantial market degradation, halting further advancement
*BLUE highlights* where there is a demonstrable, substantial market failing and further advancement is profoundly questionable

| | Property | ECC | RSA | AES | QWYIT™ |
|---|---|---|---|---|---|
| | System Type | Public Key | Public Key | Secret Key | Secret Key |
| | Key Size (bits) | 160 | 2048 | 128/192/256 | 1-256 |
| | Key Increases | YES – in bytes | YES – in blocks | NO | YES – in bytes |
| SPEED | Strength (bits) [1] | Would be 512 | Would be 15,360 | 128/192/256 | 256 |
| SPEED | Performance (Auth)[2] | 65.4x *slower* | ~54,000x *slower* | -- | Already provided |
| SPEED | Performance – (Encryption)[3] | -- | -- | 57 Steps | 4 Steps |
| EFFICIENCY | Variable keys | NO | NO | NO | YES[4] |
| EFFICIENCY | Key Updates | Manual/Sent | Manual/Sent | Manual/Sent | Auto/Nil communication[5] |
| EFFICIENCY | Library Size[6] | 39,000 SLOC | 39,000 SLOC | 39,000 SLOC | <500 SLOC |
| EFFICIENCY | TLS 1.3 Msg Overhead | ~4-7KB | ~4-7KB | -- | <1KB |
| EFFICIENCY | TLS 1.3 # of Msgs | 2 Round Trips | 2 Round Trips | -- | 1 Round Trip |
| EFFICIENCY | TLS 1.3 Process Time[7] | 112ms | 112ms | -- | <1ms[8] |
| FLEXIBILITY | TLS Initial Mutual Authentication | YES (*If* client has a certificate) | YES (*If* client has a certificate) | -- | YES, Always |
| FLEXIBILITY | TLS Continuous Mutual Auth[9] | NO | NO | -- | YES, Always |
| SECURITY | Provably Secure[10] | NO | NO | NO | YES |
| SECURITY | Quantum-safe | NO | NO | NO | YES |

[1] Equating public key length strengths (protection) to secret key length strengths – then Authentication and Encryption both equally protected – PKI will *never be strong enough*
[2] Equating PKI processing times required to provide the same strength (protection) across the Authentication methods – PKI methods will *never be fast enough*
[3] Equating *execution steps* – CPU/byte measurements are arbitrary, therefore meaningless. Cycles/step (and instructions/step) differences are configuration dependent. The bottom line on performance: Qwyit™ (256 bits) performs a single 'round' of 4 instructions, while AES-256 performs key expansion+14 rounds of 4 instructions each (57 total steps)
[4] No other method can vary the key size in-use; it's a substantial advantage: any msg length in any system at static (periodic)/random/pseudo-random (key value based) intervals
[5] Qwyit participants can update their keys to completely new, unique, random versions *without any sent communication.* This is the Holy Grail of key management.
[6] Value listed is for wolfCrypt, one of the *smallest available that supports* PKI and encryption implementation – *others are substantially larger*. Current libraries
[7] These are averages across different H/W configs, to establish an initial TLS 1.3 connection (latest version, Aug 2019)
[8] Processing a complete QwyitCipher™ exchange between any two endpoints is measured in microseconds, several orders of magnitude improvement
[9] Qwyit™ provides mutual (all parties) authentication in *every message* – not just at session start (or even less often, as the new TLS 1.3 allows))
[10] There is only one, 100% provably secure algorithm in all of secure communication: the OTP – and Qwyit delivers it

# Additional Future Products

**Qwyit™ delivers Perfect Encryption in provably secure Authentication Security *Services***

*Patented Security Systems for specific business markets*

- **QWYITSTORE™** – *Real Time* ownership of stored participant data
- **QWYITCARD™** – Perfect credit card transaction security w/o $15B chips
- **QWYITCASH™** – Tomorrow's money: No credit cards, No readers, Buy *NOW!*
- **QWYITTALK™** – Security As A Service – A perfect TLS replication and replacement

# Technology – Validation/Verification

## Qwyit® submitted to NIST for US National Standard for Lightweight Cryptography workshop 2015

- http://csrc.nist.gov/groups/ST/lwc-workshop2015/papers/session3-dicrescenzo-paper.pdf (presented under former name "Real Privacy Management (RPM)")

## Qwyit® mathematics verified by independent cryptographic experts

- http://csrc.nist.gov/groups/ST/lwc-workshop2015/presentations/session3-dicrescenzo.pdf (analyzed herein under former name "Real Privacy Management (RPM)")

# Management Team

- **Paul McGough - Founder and *CTO***
  Telecommunications expert with over 35 years of progressively responsible experience managing IT technology teams for the development, integration, implementation and support of financial, project management, database applications and security systems. Over three decades, Paul has been an inventor, and entrepreneur while holding senior positions with AOL, CSC and SAIC, with over 10 years of highly classified government secure communication project management and software engineering. Paul McGough co-founded Qwyit® where he is CTO, Chief Scientist, and Qwyit® inventor and patent author.  Paul is an amateur champion golfer and currently lives in northern Virginia.

- **Michael Fortkort - Co-Founder and *COO***
  Chief Operations Officer, Qwyit and General Counsel. Mr. Fortkort is a registered patent and corporate lawyer who has worked with startups and technological innovators for over 25 years. A graduate of the Georgetown University Law Center (cum laude), he spent ten years with a large Intellectual Property law firm, then founded his own boutique patent firm. Prior to entering the legal profession, he worked for seven years as an engineer for the U.S. Army on communication related developments. He received a BSEE from the University of Notre Dame and an MSEE in Communications from George Washington University. He's worked with Paul and the  Qwyit technology since 1998, co-founding this iteration of Qwyit together. Mr. Fortkort also founded a transportation company (Chariots For Hire), and serves as its Chairman of the Board.

# Financial Plan

## $750K Investment (Startup – 1 year operation)

*Initiate, Staff and Operate the QwyitLab™ –*

- $450K to fund QwyitLab™ for 1 year (Product prototypes in FPGA chips, initial device IoT)
  - Hire 3 Cyber-Engineers
    - 1 H/W (QwyitChip™)
    - 1 S/W (QwyitSDK™)
    - 1 Web Programmer (QwyitKey™/QwyitTalk™)
- $150K: Sales/Marketing activities/support for 1 Year
  - Develop/create introductions/awareness in Market prospects, bringing them to the QwyitLab™, demonstrating prototype products
  - Generate/Manage licensing sales cycles
- $150K: Executive Management and Lab Build/Outfit
  - Product/prototype design
  - Lab design, materials & devices budget
  - General corporate activities
- $0-200K anticipated License Revenue and/or paid prototype development/production, Q4, Y1
- Out year anticipated Revenue potential: See Dolby Labs, and Intel chip manufacture ☺

# Current Status

Complete, multiple independent reviews provide assurance that our methods deliver to their claims and specifications

- **QwyitChip™ FPGA architecture, demos, Verilog code available**
- **QwyitSDK™ available in multiple platforms (C, C++, Java)**
- **QwyitKey™ prototype-ready with minimal effort (based on existing QwyitTalk™ key delivery prototype)**
- 12 Patents Granted (11 US, 1 Japan), other patents pending
- 30+ White Papers (technology, application, marketing, documentation)
- Reference Software (test vectors, bias testing, primitives)
- 7 different example (historical) applications

# Qwyit™ Summary

- Qwyit LLC:
- Has the Technology: patented, superior, proven, products (H/W, S/W)
- Has the Market model: Initially, QwyitChip™/QwyitSDK™, FPGA-centric
- Has the Market plan for proliferation/demonstration: QwyitLab™
- Has the Business Plan: multiple licensing models (unit based, flat fee, use based, etc.)
- Has a wide open marketplace: H/W security is the answer, demanding new solutions
- Has capable, competent, expert Leadership

- All we're missing:
- The funding to staff the QwyitLab™ – to obtain Prospect/Customer feedback to finalize the initial QwyitChip™ FPGA-product design/build, and demonstrate market-based prototypes for license, manufacture and partnerships

# Opportunity

**Qwyit LLC needs a technology/business/investment partner**

**Contact PaulM@qwyit.com**

All truth passes through three stages. First, it is ridiculed. Second, it is violently opposed.

Third, it is accepted as being self-evident. - Arthur Schopenhaue