Qwyit™ Universal Encryption Dynamic Security

This document provides an introduction to the market-changing potential delivered by the world's fastest Universal Encryption engines: QwyitChip™ for H/W, the accompanying identical S/W QwyitSDK™, and QwyitKey™, the Anonymous Authentication Service. The examples mentioned here demonstrate today's Multidimensional Network inter-operability and show the need for the introduction of a new security concept: *Dynamic Security*. This doesn't mean varying levels of protection – it means delivering dynamic, on-the-fly new authentication and data encryption whenever/however the network demands – including static interactions, next-gen interactions and even new demanded and defined AI-driven on-the-fly instant interactions: all with provably secure connections.

The following are based on the full Qwyit protocol as outlined in the current version of the *Qwyit Protocol Reference* document, available from Qwyit LLC. QwyitChip™ client demo APIs are available from Qwyit LLC; go to www.qwyit.com.

Introduction

It's been a while since the press was all over the Trolley Problem for autonomous cars; AI now seems inevitable in our daily lives. What this means, is that AI will be a prominent component of network analytics, storage, and communications. But there's a missing ingredient:

How do we secure all of this important, life-changing intelligence? There's one thing about Human Intelligence that is positively guaranteed: if there's value somewhere, someone's going to try to take it 'the easy way': fraud, intrusions, impersonations…cybercrime. As networks are growing, becoming multidimensional, integrated and omnipresent, the current security models are *not* working. It's terrifying that when AI takes hold, the consequences of the lack of security won't just be annoying, they'll be catastrophic: a pandemic of cybercrime. And the worst part? There isn't a single authentication and data encryption method capable of delivering AI's participation requirements:

- It's everywhere
- It's always on
- It's provably secure – and quantum safe
- It's fast
- *It's dynamic*

Everywhere is efficient. Always on is mutual and continuous. Provably secure and quantum safe is a true, mathematic insolvability. Fast is no degradation/interruption. All of these are Qwyit™ – we've shown this in our design, our papers. But what is *Dynamic Security?* Multidimensional networks representing ever-growing and changing processes must not be limited by security techniques.

Dynamic Security is the ability for any network infrastructure, operators and participants to instantly create new authentic and encrypted connections, storage and communications.

Inclusive of the properties of efficiency, continuous, provably secure and speed, *Dynamic Security* requires that security is in waiting without being 'established' or 'formal' or 'defined'. It is exactly the same as how all of the different components of the human brain are ready to 'do intelligence'. One

isn't limited by first having to grow new cells, teach them how to talk to one another, etc.: our brains just *work*. And AI does exactly the same thing: it learns and then performs.

Can you imagine having to limit AI in networks the way we limit employees by first sending them to 'security training'…so they can *fit into the security models, instead of fitting the security models into their innovation?*

It's one thing to exercise control over employees through tedious business processes and human resource office requirements; AI in networks simply will not work without *Dynamic Security*.

Dynamic Security – What it looks like

Here's a current article (3/2020) about Waymo's autonomous cars:

https://cleantechnica.com/2020/03/07/waymo-unveils-its-5th-generation-autonomous-driving-technology/

The first, most noticeable aspect of the entire system of hardware (lidar, radar, cameras, etc.) and software (control, analysis, interaction, etc.) is the *complexity*. Complexity isn't a good thing for today's security methods: they're already too complex and overstuffed themselves, so the resulting *total security of the car is almost nonexistent:* they can and will be hacked – for every possible reason (theft, misuse, crime against the passengers (rerouting/stalling/stopping vehicles, etc.), etc., etc.

Solving this insecurity is 'regular Qwyit': implementing in the same manner/locations/processes as the current methods, but with superior properties (speed, efficiency, provably secure, etc.). But that only brings the car's total security up to *poor* by protecting the general aspects of autonomous driving (routing S/W, owner control S/W, etc.) This kind of protection is akin to the current 'general' protection provided to digital networks: there's still an escalating cybercrime rate of over 30%!

The car can be hacked in all the places where there is no security: the actual H/W devices (individual cameras, lidar, etc.), and the internal S/W processing of the autonomous capability. [Remember the casino hack through an aquarium tank thermometer?!] Not only does this require protection, but it requires *Dynamic Security*. The entire system will be constantly updated, learning, improving response rates, acquiring new skills that encompass more and more of the autonomous mission: traffic control integration, business system's integration/involvement for purposing the car trips, app S/W for human enterprise/innovation/use ("Gee, we never thought people would use the cars *that way!*"), etc.

Here's what Dynamic Security looks like in autonomous cars: *All of the 'etcetera's' in the preceding will change the way 'The Security' will/should/might/could work!* These ***can't*** be limited by security methods. If they are, people's lives are at stake. If someone's child is killed in a hacked autonomous vehicle because 'they couldn't secure all of the complexity', the lawsuits will terminate the entire technology sector – like Vioxx, Accutane, etc. Technology has never been in the forefront of successful marketplace products that fail terminally because they caused human tragedy – if Dynamic Security isn't a part of autonomous driving, it will be.

There are many, many more examples of systems requiring Dynamic Security:

- IoT smart systems – "Why do I have to wait until Amazon adds a security capability between my Alexa and my new smart hub geothermal heat pump? Can't I do that myself by asking it to connect? That's what 'smart' means, doesn't it?!"
- Telecommunications systems – "I just want to call people securely. Text them privately. Why on earth should I have to buy a particular phone, use a specific app – and get my friends to do the same?! *I just want it all to be private!*"
- The Internet – "This browser…that browser. This site…that site. I hear *every day* that they're reading my brain!! Don't I have a *Right To Privacy in The Information Age?!*"

In all of these examples, there is commonality in the reason behind the end user's exasperated interpretation of the failing in these systems' purposes: Security doesn't exist, it isn't spontaneous, *and they have no control over it*. Current methods aren't working, don't fit, won't *ever* fit and work – *and have never been capable of true end-user control*.

But there *is* a solution: Qwyit's new Universal Encryption engines: QwyitChip™/QwyitSDK™*,* used in the QwyitKey™ key distribution system, is the World's First and Only *Dynamic Security* system. It will finally deliver on the user's security expectations, demands – and rights.

Dynamic Security – How it works, Part 1: Authentication

Logically, the only way for an end-user to be in control of their own data/information, and therefore in control of the security, is to create their own keys. All digital systems require authentication and encryption 'keys' – whatever form they take. Every message sent has to perform/contain both. In today's digital systems, authentication is performed by trusted 3rd Parties. These were introduced by the proliferation of Public Key Infrastructures over the last 50 years, and they became responsible for generating/holding a portion of the key structure (the certificate) for authentication purposes; and therefore they became 'in control' of the security. Not only was this because of the complexity of the public key math, but the PKI trust model mandated it.

PKI 3rd party trust models dictate that you'll show your security membership credentials by holding a certificate with them – that they created just for you, and that you can share w/your intended recipient if asked – but the messages don't go through that 3rd party: you trust the *math* of the certificate creation, and the holder of it. It's like the Hotel California – you can get a new certificate any time you like, but it's never yours!

Qwyit® has developed a new trusted 3rd party called QwyitKey™, which provides participant–managed, independent trust. In the QwyitKey trust model, you'll show your security membership credentials by having a unique relationship with the service (your shared QwyitKey secret key), and you'll pass every message *through that relationship relying on your intended recipient's unique relationship with the service*.

The crucial difference between these 3rd party trust models is ownership of the authentication. With PKI, the 3rd party owns the public trust as if they are a part of your purpose group: *but they never are!* In QwyitKey, the 3rd party doesn't own the public trust, they simply vouch for the public *route every time you travel (message) – YOU own/earn the trust of each individual recipient in your purpose group when you arrive and get private.*

The difference is as if when you get in a car to go visit your friend, every time you start the car you have to check in with the government using PKI, and your friend has to open the door and let you in believing the government's identification that you're you – but in QwyitKey, you simply follow all the traffic rules to arrive safely, then your friend authenticates you before they open the door.

It's obvious in today's multidimensional networks, you simply can't have 'the government' be a part of the architecture: that autonomous car will kill you when fraudulent authentication takes over the driving.

Dynamic Security *requires* participant-managed, independent trust in order to operate.
Current systems *will never be able to provide Dynamic Security.*

Dynamic Security – How it works, Part 2: Encryption

QwyitKey provides the proper authentication trust model and operational capability to deliver participant-managed keys allowing trusted Dynamic Security (DS). But that's only half the story: now we've got to enable the use of those keys to encrypt all of the digital traffic…dynamically! Logically, this requires an encryption capability *everywhere*. Not only does this tighten the massive security holes in current practice (thermometer doorways!), but it allows the core DS mission: instant, new, simple pathways to deliver total security. If every 'network place' (devices, switches, S/W, etc.) has the ability to use their own keys to securely encrypt traffic in any network pathway (including creating new ones), the system becomes possible, flexible, impenetrable; exactly what those end users expect.

[There is one important aspect to remember about all these 'participants' – they don't *all* have to be able to *connect* to the QwyitKey service; they simply have to belong. As mentioned in the *QwyitKey™ Reference Guide*, there are various ways to accomplish this, including manufacturer pre-set keys, etc.]

Obviously, there are a few absolute requirements for putting 'security everywhere', the ability to encrypt everything using participant-managed keys. The encryption/decryption 'engine' must be:

- *Fast* – within the operating tolerances of the communications' protocols such that there is no limit to the number of times traffic is encrypted/decrypted; and new routes aren't introducing degradation
- *Small* – so tiny within the space tolerances of current H/W specs that they can be put anywhere, everywhere w/o limitation
- *Universal* – the enc/dec method has to be exactly the same everywhere; H/W, S/W, anywhere/everywhere the engine exists
- *Future Assured* – provably secure now and Quantum safe forever

Another reason those autonomous cars don't have Dynamic Security is because there isn't a single current encryption method that comes close to those requirements – and none of any of the proposed 'new' methods (such as those being presented as *Quantum Safe*) will either.

Luckily, QwyitChip™ and QwyitSDK™ *do* meet them – completely and to the extent that nothing will ever be needed to 'improve' them: they are perfect today, and tomorrow. *They are already Quantum Safe!*

Dynamic Security – How it works, Part 3: The Vision

Every great global technology leap was preceded by a period of fits and starts; where most of the pieces existed, innovative people were attempting different things, and just over the horizon looked wonderfully exciting. But everyone knew something was missing – some particular bit of innovative technology. As soon as it appeared, everything changed, and a tech boom was born:

- The horse and buggy was around…until the Car!
- The Internet was around for 20 years…until the World Wide Web!
- Mobile communications were around…until the Smart Phone!
- Artificial Intelligence is around…

…Until it is *trusted*. Qwyit® is the innovative technology that will let it explode.

The potential of today's multidimensional networks, such as an AI autonomous traffic system (much more than just *cars*), will *never* be reached until it can be controlled and trusted. All of the Cambridge Analytica-type issues, the privacy wars being waged, the trepidation behind Artificial Intelligence – all of these *can be mitigated by proper implementation of the security of the systems. Current methods will never provide the requisite trust* – the simple proof is in the complete lack of it anywhere today: no one building the networks, the apps, the next generation computing puts them in. They don't know how they work (complexity), they don't fit (efficiency), they don't apply (flexibility), they take too much time (speed)…and *none of it will ever work dynamically.*

Qwyit® has the simplicity, the efficiency, the flexibility, *the speed* – and, as shown above with the proper Authentication and key distribution (QwyitKey) and built-in encryption everywhere (QwyitChip™ and QwyitSDK™), Qwyit® has what it takes to deliver Dynamic Security.

Conclusion

Qwyit® understands that those exploding new technology frontiers don't happen overnight. We're ready to work with all parties to proliferate our Dynamic Security solution; because it's absolutely necessary to realize the multidimensional network potential. Those autonomous cars need protection now, and they'll need improving S/W control applications that will have to work with the existing H/W – the security must be 'baked-in'. The pieces of the DS constantly changing puzzle can't be hindered by security techniques – the techniques need to be universal, the H/W needs to already be complete, efficiently configured for dynamic control – and provably safe.

It's only a matter of time before the coming AI revolution…Qwyit's ready to deliver the necessary security: We have backing, serious innovation, a solid proof of concept and the digital world is aching for privacy.

When this is available – when Qwyit's Universal Encryption Dynamic Security platform of QwyitKey, QwyitChip™ and QwyitSDK™ are everywhere – the overwhelming tide of cybercrime won't exist; and there'll be a real trustworthy balance of digital privacy, security, ownership, performance and safety. Today…and in the dynamic future!