QwyitStore™ Overview

The QwyitStore™ Data Storage and Access Control *Service* (QwyitStore™ *Storage as a Service*) is an unbreakable data storage and identifiable access and use control service. Qwyit provides features, benefits, authentication and data security (stream cipher) for data storage using the Qwyit Directory Service (QDS) key store. QwyitStore™ (QS™) is an implementation capability based on the full Qwyit protocol as outlined in the current version of the *Qwyit Protocol Reference* document, available from Qwyit LLC. QS™ requires all participants, and uses the core messaging systems of, QwyitTalk™ *Security as a Service* available at Qwyit.com. Please see the *QwyitTalk™ Reference Guide* for details. *The QwyitStore™ Reference Guide* and client demo APIs are available; go to www.qwyit.com.

Why QwyitStore™

As of this writing (4/2018), there is a confluence of events occurring associated with individual privacy concerns, rights and 'downstream' control of personal digital data given to public entities. Mark Zuckerberg of Facebook appeared before the US Congress to testify about public corporate responsibility for customer's private data. There are wide-ranging new European Privacy laws that will become effective within the next month. And several perspectives are being presented throughout technology and mainstream media about 'The Answers' to 'This Problem'.

Unfortunately, not only is the problem undefined, there aren't any actual technical solutions other than to 'trust' that the data holder will 'act properly' and somehow, 'keep the data private.' Obviously, this isn't good enough. Nor is it enough to simply enact laws that are easily avoided by entities claiming that they meet the legal standards because they 'perform Best Practices' when there are none. This is why QwyitStore™ is presented: To give a clear, unbreakable technology solution that can be easily implemented by any data holding entity that provides a clear, secure and private capability to the actual data owner, The Private Digital Citizen. QS™ also delivers a realistic 'Best Practice' means for the data holder to abide by not only the intent of the laws, but the discernable act of compliance.

Digital Data Storage Defined

The beginning of data storage: you have information. If you're the only recipient of this information, it's fairly easy to 'keep it secret': store it in your head! Even if it's a lot of data, you can store it in a form that no one else can recognize; and if it's stored digitally, that means you encrypt it. And only you have the key…in your head, or someplace only you know. Done.

But what if you need to share this information with another party, person, entity, etc.? Now how do you do it? Store it at your place, and give them a copy of the key? There are cool cryptographic ways for you to give them a 'sorta same' key that's not the original key that they can use. And you can even set it up to alert you if/when one of your authorized key-holders accesses the data – you could even segregate the encrypted content by different keys, and then they only grant access to specific data. Again, Done.

But what's real world: you have information *that other parties want to use at their places, in their processes, with their authorized parties.* Uh-oh. You can't get to 'Done'. Not ever, because there is a fundamental problem, as well as two inherently different 'collections' of your private data:

The Fundamental Storage Problem

You/me/all of us ***don't have Decryptors in our heads!*** So after you create your data, and you give it to another party to use, even if they store it with unbreakable encryption…eventually, someone will *see it, hear it, read it.* And somewhere between its encrypted state and the person's eyes/ears/head, it will be unencrypted…and *right then*, it can be stolen, copied, forged…*not* Done! This Fundamental Storage Problem can*not* be solved. Oh sure, we can build robot-heads that can read it from its digitally encrypted state…but even these will have to *decrypt it eventually, somewhere* to compare whether it's authentic or not…and criminals can build fraudulent robot-heads to steal it!

This problem can *only be mitigated*. And the perfect way to do that, is to enable unbreakable access control – so you know who you authorized to view/use your data…and post-authorization, if the data appears anywhere, at minimum, you'll have recourse. There is one, quite large, exception to this mitigation: you allow the same data to be stored in multiple places…then even if you know who you last authorized to view/use it, *it could still have been one of the other's fault, error, mistake*.

These two, make up the FS Problem. QwyitStore™ will provide mitigation through unbreakable Access Control, as this is the best possible solution that can be offered.

The Equifax Problem

On 9/7/2017, credit monitoring company Equifax announced that 140*million* personal data records were stolen. Afterwards, the number moved up another 2.5*million*. This is just one of the last decade's worth of stolen personal data fraud/theft incidents – it is a regular occurrence. These thefts are the result of a fundamental problem with data storage revolving around *ownership* and *data element value*.

First, you/we/all of us gave Equifax (et al) our data with the expectation that *they* would control it for us – it is, after all *our data*. Oops. They didn't. Whatever systems' they all used were faulty for one single reason: *our data was not end-to-end secure, i.e. encrypted.* This can't be understated: In order to steal 140*million* records, criminals should have to go to *140Million Different Places*. This is a simple thing to understand: Big Bank doesn't keep its *$Billions* in a single *place*. Equifax, because it is a single entity providing *millions* of data elements to *millions* of places that use it, should have had *you store it there encrypted*, then just be responsible for *controlling the access to it with an unbreakable communication process where it is singly decrypted for every use*. End-To-End encrypted control by the actual owner solves this EP. Done.

Second, the *Equifax Problem* revolves around *unique data elements of differing value*. For instance, your Social Security Number is extremely valuable. Your address is not. *The data collection process should be specifically designed to provide unique encryption parsed by data element value*. In concert with the ownership solution where *you* end-to-end control the encryption, this works in with mitigating access control issues.

The Facebook Problem

If you use Social Media, and other large destination websites of any kind, there is a specific type of knowledge available in all of the sporadic, varying, changeable data you provide: *The Collection*. Most

of your data is meaningless…until it is collected together. Then it has lots of different types of *value*: in comparison with others, in stratifying your 'social status' (big house, car, $$, etc.), in collating your personal habits (what, when, how you buy, when you're home, etc.) – etc., ETC.! This collection *seems* difficult to encrypt. It is intermingled with others' data, you want access to it without bother, etc. So how does *QS*™ solve this *Facebook Problem?*

The short answer – we don't. Facebook, et al, need to. Their short answer: as a user/member/somehow registered participant of their services, *they identify you at the start of every session*. Everything that happens after that, is Your Record. Whether or not they have 'issues' with the way they've built their backend systems to store *your* data based on a new requirement that *you impose on them in order to use their services* is irrelevant. This is called 'The Customer Is Always Right' mixed with 'Voting With Your Feet': if they can't provide QS™ protection to all of your data because they can't meet a new requirement – *a new entity will.*

We most certainly could implement a 'new' trust model for a specific QS™ based on each of these *Collector's* needs – but since everything Qwyit does is uniform, universal, unbreakable and specifically designed, built and operated for the benefit of *the individual digital citizen drifting amidst a public sea of digital humanity*, it is best to leave implementation to the Collectors. This way, you'll know just where to go to get resolution to any inappropriate access and/or use of your private data.

How QwyitStore™ works

The QwyitStore™ consists of three main entities, with a possible subset number of additional authorized parties:

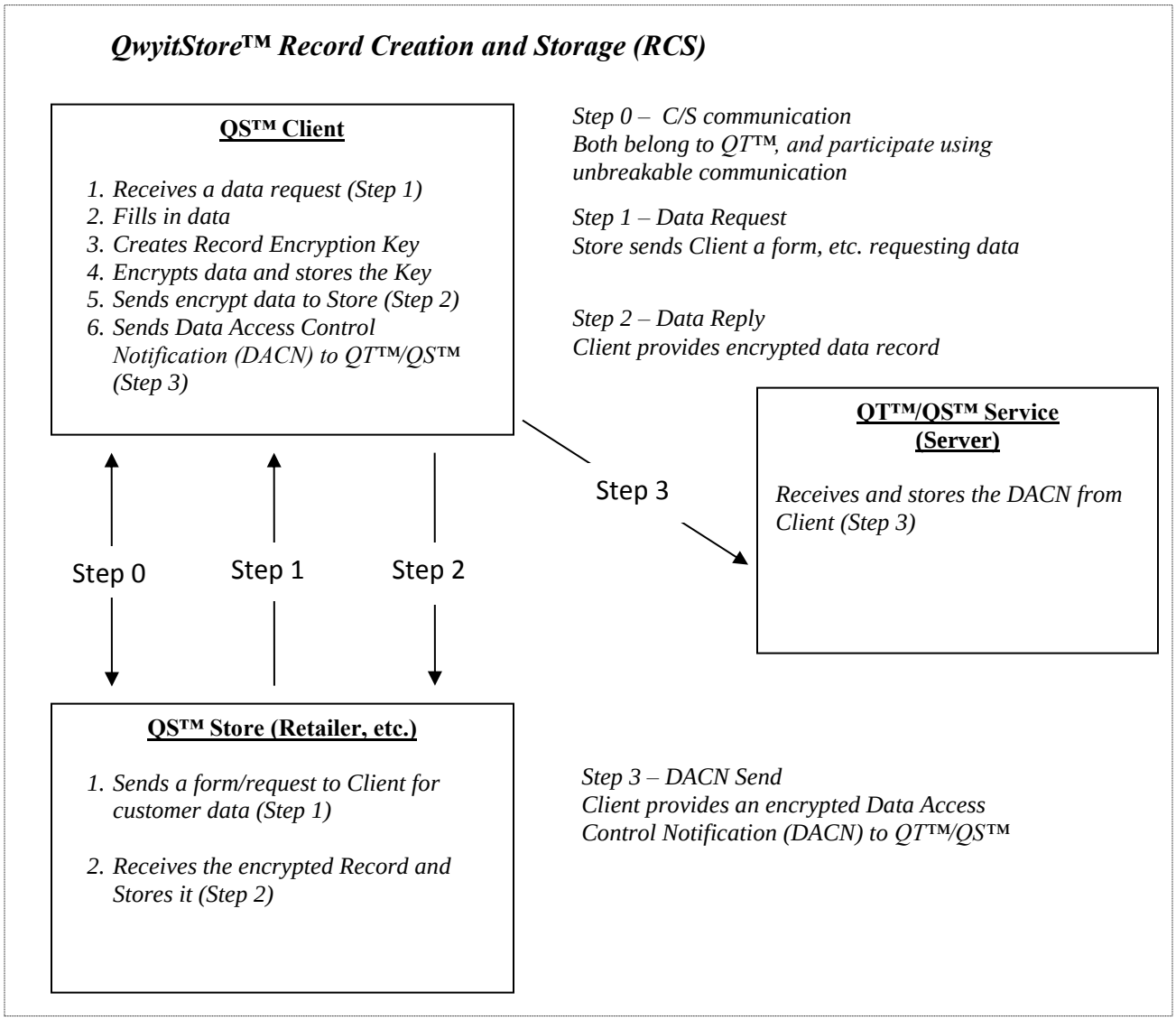
1. QwyitStore™ Service
    a. This is server provision of the QS™. It is available in concert with, and performs like, the QwyitTalk™ Security as a Service communications security service available at Qwyit.com
2. QS™ Store
    a. This is any entity that will need/want/offer to keep personal data
    b. Additionally, the Store may authorize (through a sale, partnership, etc.) additional 3rd Parties who will have the original, have access to the original or store copies of this personal data
3. QS™ Client
    a. Any QS™ participant who provides personal data, and wishes to maintain its security as well as control its access

There are two QS™ processes:

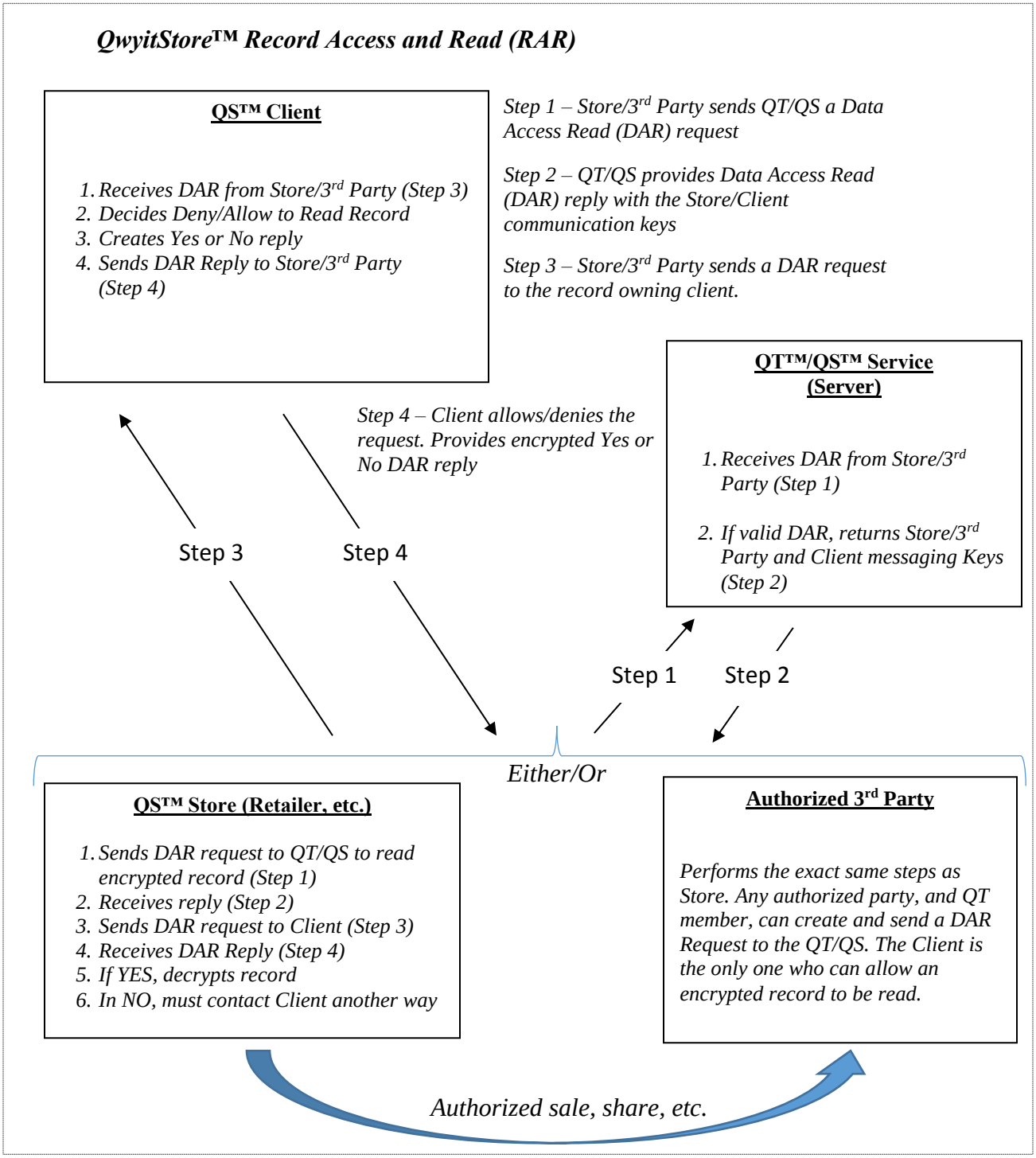
- Record Creation and Storage (RCS)
    - This is Client receipt of a request from the Store/3rd Party for data, Client supplies data, and encrypts the record, which is returned to the Store
- Record Access and Read (RAR)
    - This is Store/3rd Party request to read the encrypted Client record at the QT™/QS™, unbreakable notification to the Client, Client provision of the record encryption key to the Store/3rd Party if decided it is appropriate (delivered in encrypted form), Store/3rd Party uses the key to view and process the record. The record is *never* allowed to be additionally/separately stored in decrypted form

Participation by any Store and 3rd Party in the QS™ Service will require licensed grant that no record or any portion will ever be stored other than in the encrypted form received from any Client. Client reliance on this agreement should be accompanied by substantial and well defined legal remedy.

The following are the overview diagrams of the two processes in plain English – these same diagrams are well defined in the accompanying *QwyitStore™ Reference Guide*:



QwyitStore™ Record Access and Read (RAR)



Conclusion

There are currently no formal, universal, uniform end-to-end encrypted data storage systems available to individual digital citizens. QwyitStore™ provides unbreakable communication between real world digital entities and a simple, efficient mechanism to deliver private unbreakable storage in an end-to-end manner; as well as conclusive access control over stored encrypted records.

While no encrypted storage system can solve the Fundamental Problem, QS™ provides the maximum possible mitigation in combination with provably secure storage solving both the Equifax and Facebook Problems. QwyitStore™ finally delivers a 'Best Practice' tool for both the law-beholden data collection entity, the trusting Private Citizen, and fully meets the legal community standards – and expectations – for digital privacy and security.

For the complete technical QS™ implementation details, see *The QwyitStore™ Reference Guide.*